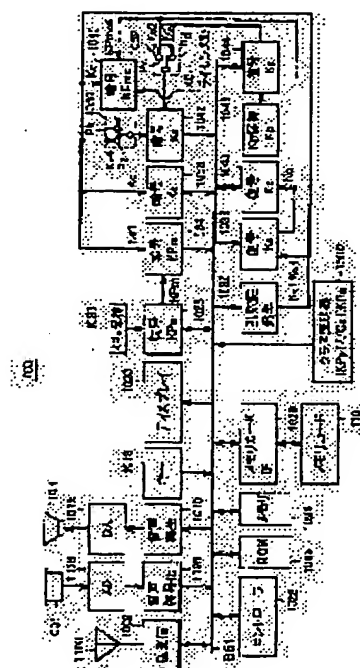


(11)Publication number : 2003-022219  
(43)Date of publication of application : 24.01.2003 .

G06F 12/14  
G06F 15/00  
G06F 17/60  
H04L 9/08

(72)Inventor : HORIUCHI KEIJI  
YOSHIKAWA TAKATOSHI  
HIOKI TOSHIAKI  
HORI YOSHIHIRO

**SOLUTION:** In a portable telephone set 100, a controller 1022 stores contents data and additional information received from a distribution server in a memory 1024. At the time of transmitting the contents data to a memory card 110, a random number key generating part 1032 generates a license key, and an encryption processing part 1034 encrypts the contents data by using the license key. The controller 1022 transmits the encrypted contents data through a memory card interface 1026 to the memory card 110. Then, the controller 1022 erases only the contents data stored in the memory 1024.



[Date of request for examination]  
[Date of sending the examiner's decision of rejection]  
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]  
[Date of final disposal for application]  
[Patent number]  
[Date of registration]  
[Number of appeal against examiner's decision of rejection]  
[Date of requesting appeal against examiner's decision of rejection]  
[Date of extinction of right]

05/10/26

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-22219

(P2003-22219A)

(43) 公開日 平成15年1月24日 (2003.1.24)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
			3 2 0 D 5 B 0 8 5
15/00	3 3 0	15/00	3 3 0 Z 5 J 1 0 4
17/60	1 4 2	17/60	1 4 2
	3 0 2		3 0 2 E

審査請求 未請求 請求項の数25 O L (全 31 頁) 最終頁に続く

(21) 出願番号 特願2001-207428(P2001-207428)

(22) 出願日 平成13年7月9日(2001.7.9)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 発明者 堀内 啓次

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(72) 発明者 吉川 隆敏

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(74) 代理人 100064746

弁理士 深見 久郎 (外3名)

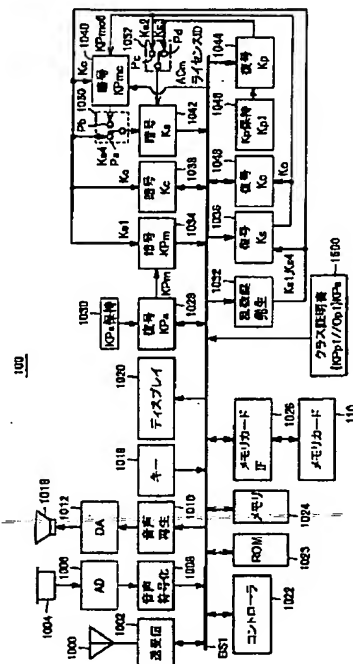
最終頁に続く

(54) 【発明の名称】 コンテンツデータを容易に再取得できるデータ端末装置、その端末装置において実行されるプログラム、およびそのプログラムを記録した記録媒体

(57) 【要約】

【課題】 取得したコンテンツデータを他の装置へ送信するときに削除しなければならないコンテンツデータの流通を著作権を保護しながら促進するデータ端末装置を提供する。

【解決手段】 携帯電話機100においては、コントローラ1022は、配信サーバから受信したコンテンツデータおよび付加情報をメモリ1024に記憶する。そして、コンテンツデータをメモリカード110へ送信するとき、乱数鍵発生部1032は、ライセンス鍵を生成し、暗号処理部1034は、コンテンツデータをライセンス鍵によって暗号化する。コントローラ1022は、暗号化されたコンテンツデータをメモリカードインタフェース1026を介してメモリカード110へ送信する。そして、コントローラ1022は、メモリ1024に記憶されたコンテンツデータのみを削除する。



## 【特許請求の範囲】

【請求項 1】 平文のコンテンツデータを取得して前記コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを復号するためのライセンス鍵とを生成し、前記コンテンツデータの付加情報と、前記生成した暗号化コンテンツデータおよびライセンス鍵とをデータ記録装置との間で送受信するデータ端末装置であって、

指示を入力するための操作部と、

前記データ記録装置との間でデータをやり取りするインタフェースと、

前記平文のコンテンツデータおよび前記付加情報を記憶する記憶手段と、

前記ライセンス鍵を生成し、その生成したライセンス鍵によって前記コンテンツデータを暗号化して前記暗号化コンテンツデータを生成する暗号化コンテンツ生成手段と、

前記ライセンス鍵を含み、かつ、前記データ記録装置から前記ライセンス鍵が出力されたとき前記データ記録装置に記録された前記ライセンス鍵を前記データ記録装置において実質的に削除するためのライセンスを生成するライセンス生成手段と、

前記ライセンスを暗号化した暗号化ライセンスを生成する暗号処理手段と、

制御手段とを備え、

前記制御手段は、前記操作部を介して入力された前記コンテンツデータの前記データ記録装置への送信要求に応じて、前記平文のコンテンツデータおよび前記付加情報を前記記憶手段から読出し、その読出したコンテンツデータを前記暗号化コンテンツ生成手段に与え、前記暗号化コンテンツデータ、前記暗号化ライセンス、および前記付加情報を前記インタフェースを介して前記データ記録装置へ送信し、前記記憶手段に記憶された平文のコンテンツデータを削除し、

前記付加情報は、前記コンテンツデータの取得元にアクセスするためのアクセス情報を少なくとも含む、データ端末装置。

【請求項 2】 前記記憶手段は、

$n$  ( $n$  は自然数) 個のコンテンツデータを記憶するデータ領域と、

前記データ領域に記憶されているコンテンツデータに対応して、前記コンテンツデータの存在位置と、前記コンテンツデータの削除を示す  $m$  ( $m$  は  $m \geq n$  である自然数) 個のリスト情報とを記憶するリスト領域とを含み、前記制御手段は、前記コンテンツデータを前記データ記録装置へ送信したとき、前記送信したコンテンツデータに対応する前記リスト情報を更新する、請求項 1 に記載のデータ端末装置。

【請求項 3】 前記制御手段は、前記操作部を介して入力された前記コンテンツデータの再生要求に応じて、前

記リスト領域に記憶されたリスト情報を読出し、その読出したリスト情報に基づいて前記再生要求されたコンテンツデータが前記記憶手段に記憶されているか否かを検索し、前記再生要求されたコンテンツデータが前記記憶手段に記憶されていないとき、前記付加情報に含まれる前記アクセス情報に基づいて前記再生要求されたコンテンツデータを再取得する、請求項 2 に記載のデータ端末装置。

【請求項 4】 前記制御手段は、前記付加情報を前記コンテンツデータとともに取得し、その取得した付加情報を前記リスト領域に格納し、前記取得したコンテンツデータを前記データ領域に格納する、請求項 2 または請求項 3 に記載のデータ端末装置。

【請求項 5】 前記制御手段は、前記コンテンツデータを取得すると、その取得したコンテンツデータのリスト情報を作成し、その作成したリスト情報を前記リスト領域に格納する、請求項 2 または請求項 3 に記載のデータ端末装置。

【請求項 6】 前記制御手段は、前記コンテンツデータを取得するとき、その取得するコンテンツデータに対応する付加情報が存在するばあい、前記付加情報を取得せず、前記コンテンツデータのみを取得する、請求項 2 から請求項 5 のいずれか 1 項に記載のデータ端末装置。

【請求項 7】 前記ライセンス生成手段は、前記暗号化コンテンツデータを復号および再生する回数を 1 回に設定した再生条件と、前記ライセンス鍵とから前記ライセンスを生成する、請求項 1 から請求項 6 のいずれか 1 項に記載のデータ端末装置。

【請求項 8】 前記暗号化コンテンツ生成手段は、

前記ライセンス鍵を生成する鍵生成部と、

前記ライセンス鍵によって前記コンテンツデータを暗号化する暗号処理部とを含む、請求項 1 から請求項 7 のいずれか 1 項に記載のデータ端末装置。

【請求項 9】 前記暗号処理手段は、前記データ記録装置から受信した第 2 のセッション鍵によって前記ライセンスを暗号化する、請求項 1 から請求項 8 のいずれか 1 項に記載のデータ端末装置。

【請求項 10】 前記データ記録装置との通信を特定するための第 1 のセッション鍵を生成するセッション鍵生成手段と、

前記第 1 のセッション鍵によって暗号化されたデータを復号する復号処理手段とをさらに備え、

前記ライセンスの前記データ記録装置への送信時、

前記セッション鍵生成手段は、前記ライセンスの前記データ記録装置への送信を特定する第 1 のセッション鍵を生成し、

前記制御手段は、前記第 1 のセッション鍵を前記インタフェースを介して前記データ記録装置へ送信し、前記第 1 のセッション鍵によって暗号化された前記第 2 のセッション鍵を前記インタフェースを介して前記データ記録

3

装置から受取り、その受取った前記第1のセッション鍵によって暗号化された前記第2のセッション鍵を前記復号処理手段に与える、請求項9に記載のデータ端末装置。

【請求項11】 前記データ記録装置との通信を特定するための第1のセッション鍵を生成するセッション鍵生成手段と、

前記第1のセッション鍵によって暗号化されたデータを復号する復号処理手段とをさらに備え、

前記暗号処理手段は、

前記データ記録装置に固有な第1の公開暗号鍵によってデータを暗号化する第1の暗号器と、

前記データ記録装置において生成された第2のセッション鍵によってデータを暗号化する第2の暗号器とを含み、

前記制御手段は、前記第1のセッション鍵によって暗号化された前記第2のセッション鍵と前記第1の公開暗号鍵とを前記データ記録装置から前記インタフェースを介して受け、その受けた前記第1のセッション鍵によって暗号化された前記第2のセッション鍵と前記第1の公開暗号鍵とを前記復号処理手段に与え、前記復号処理手段によって復号された前記第1の公開暗号鍵を前記第1の暗号器に与え、前記復号処理手段によって復号された前記第2のセッション鍵を前記第2の暗号器に与え、前記第1の暗号器は、前記ライセンスを前記第1の公開暗号鍵によって暗号化し、前記第2の暗号器は、前記前記第1の暗号器の出力を前記第2のセッション鍵によって暗号化して前記暗号化ライセンスを生成する、請求項1から請求項8のいずれか1項に記載のデータ端末装置。

【請求項12】 第2の公開暗号鍵によってデータを暗号化するもう1つの暗号処理手段をさらに備え、前記制御手段は、前記データ記録装置から前記第2の公開暗号鍵を含む認証データを前記インタフェースを介して受け、その受けた認証データが正当であると判断したとき、前記受けた認証データに含まれる前記第2の公開暗号鍵を前記もう1つの暗号処理手段に与え、前記もう1つの暗号処理手段において前記第2の公開暗号鍵によって暗号化された前記第1のセッション鍵を前記インタフェースを介して前記データ記録装置へ送信し、前記もう1つの暗号処理手段は、前記セッション鍵生成手段によって生成された前記第1のセッション鍵を前記第2の公開暗号鍵によって暗号化する、請求項9から請求項11のいずれか1項に記載のデータ端末装置。

【請求項13】 前記データ記録装置に対する認証データを保持する認証データ保持部をさらに備え、

前記制御手段は、前記操作部を介して入力された前記暗号化コンテンツデータの前記データ記録装置からの受信要求に応じて、前記認証データを前記インタフェースを介して前記データ記録装置へ送信し、前記認証データが

4

前記データ記録装置において認証されると、前記データ記録装置から前記暗号化コンテンツデータおよび前記ライセンス鍵を前記インタフェースを介して受信する、請求項1から請求項6のいずれか1項に記載のデータ端末装置。

【請求項14】 前記制御手段は、前記データ記録装置において前記ライセンス鍵を実質的に削除するための処理が行なわれると、前記暗号化コンテンツデータおよび前記ライセンス鍵を前記インタフェースを介して受信する、請求項13に記載のデータ端末装置。

【請求項15】 前記暗号化コンテンツデータを前記ライセンス鍵によって復号する復号処理手段をさらに備え、

前記制御手段は、前記暗号化コンテンツデータおよび前記ライセンス鍵を前記復号処理手段に与え、前記復号処理手段によって復号されたコンテンツデータを前記記憶手段に格納する、請求項13または請求項14に記載のデータ端末装置。

【請求項16】 前記データ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成手段と、

前記セッション鍵生成手段が生成したセッション鍵によって暗号化されたデータを復号するもう1つの復号処理手段とをさらに備え、

前記コンテンツデータの前記データ記録装置からの受信時、

前記セッション鍵生成手段は、前記コンテンツデータの前記データ記録装置からの受信を特定するセッション鍵を生成し、

前記制御手段は、前記セッション鍵を前記インタフェースを介して前記データ記録装置へ送信し、前記セッション鍵によって暗号化された前記ライセンス鍵を前記インタフェースを介して前記データ記録装置から受取り、その受取った前記セッション鍵によって暗号化された前記ライセンス鍵を前記もう1つの復号処理手段に与える、請求項15に記載のデータ端末装置。

【請求項17】 前記コンテンツデータは、平文で実行可能なデータもしくはプログラムである、請求項1から請求項16のいずれか1項に記載のデータ端末装置。

【請求項18】 コンテンツデータと前記コンテンツデータを再び取得するために必要な取得情報とを外部から取得して格納し、前記コンテンツデータを利用するデータ端末装置であって、

指示を入力するための操作手段と、

前記コンテンツデータおよび前記取得情報を記憶する記憶手段と、

制御手段とを備え、

前記制御手段は、

前記操作手段からの指示に従って、前記記憶手段に記憶されたコンテンツデータを削除するとき、その削除する

コンテンツデータに対応した取得情報を保持するように前記記憶手段を制御し、

削除したコンテンツデータを利用するように前記操作手段から指示されたとき、前記記憶手段に格納されている取得情報に基づいて、前記削除したコンテンツデータを再び外部から取得して前記記憶手段に格納する、データ端末装置。

【請求項 19】 前記記憶手段は、記憶している、または記憶していた複数のコンテンツデータの記憶状態と識別情報とを含むコンテンツリストをさらに記憶し、

前記制御手段は、

前記操作手段からの指示に従ってコンテンツデータおよび取得情報を新たに取得したとき、前記新たに取得したコンテンツデータおよび取得情報を前記記憶手段に格納し、かつ、前記コンテンツリストに前記新たに取得したコンテンツデータに対応した記憶状態と識別情報とを追加し、

前記操作手段からの指示に従って前記記憶手段に記憶されたコンテンツデータを削除するとき、削除するコンテンツデータが前記記憶手段に格納されていないことを確認できるように、削除するコンテンツデータに対応する記憶状態を変更し、

前記削除したコンテンツデータを外部から再取得したとき、再取得したコンテンツデータが前記記憶手段に格納されていることを確認できるように、再取得したコンテンツデータに対応する記憶状態を変更し、

前記操作手段からコンテンツデータの利用を指示されたとき、前記コンテンツリストに基づいて、前記指示されたコンテンツデータが前記記憶手段に格納されているか否かを確認する、請求項 18 に記載のデータ端末装置。

【請求項 20】 前記コンテンツリストは、前記取得情報をさらに含み、

前記制御手段は、コンテンツデータを外部から新たに取得したとき、その取得したコンテンツデータに対応する取得情報も取得し、その取得した取得情報を前記コンテンツリストに格納する、請求項 19 に記載のデータ端末装置。

【請求項 21】 平文のコンテンツデータを取得する第 1 のステップと、

前記コンテンツデータの取得元へアクセスするためのアクセス情報を少なくとも含む付加情報と前記取得したコンテンツデータとを記憶手段に格納する第 2 のステップと、

前記コンテンツデータを暗号化した暗号化コンテンツデータを復号するためのライセンス鍵を生成し、その生成したライセンス鍵によって前記コンテンツデータを暗号化した暗号化コンテンツデータを生成する第 3 のステップと、

前記ライセンス鍵を含み、かつ、データ記録装置から前記ライセンス鍵が出力されたとき前記データ記録装置に

記録された前記ライセンス鍵を前記データ記録装置において実質的に削除するためのライセンスを生成する第 4 のステップと、

前記ライセンスを暗号化した暗号化ライセンスを生成する第 5 のステップと、

前記暗号化コンテンツデータ、前記暗号化ライセンス、および前記付加情報を前記データ記録装置へ送信する第 6 のステップと、

前記記憶手段に記憶された前記コンテンツデータを削除する第 7 のステップとをコンピュータに実行させるためのプログラム。

【請求項 22】 前記第 1 のステップにおいて、前記コンテンツデータが取得されると前記付加情報が作成される、請求項 21 に記載のプログラム。

【請求項 23】 前記付加情報は、前記第 1 のステップにおいて前記コンテンツデータとともに取得される、請求項 21 に記載のプログラム。

【請求項 24】 前記第 1 のステップにおいて、前記コンテンツデータが取得されると前記コンテンツデータの存在位置を示すリスト情報がさらに作成され、

前記第 2 のステップにおいて、前記作成されたリスト情報が前記記憶手段にさらに格納される、請求項 21 に記載のプログラム。

【請求項 25】 請求項 21 から請求項 24 のいずれか 1 項に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、取得したコンテンツデータを他の装置へ送信するとき削除しなければならないコンテンツデータの流通を著作権を保護しながら促進するデータ端末装置、プログラム、およびそのプログラムを記録した記録媒体に関するものである。

【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】また、最近では、Java (R) が携帯電話機に搭載されたことにより、ソフトウェアをサーバから受信し、その受信したソフトウェアを用いて各種の画像データを携帯電話機の表示部に表示することができるようになった。さらに、携帯電話機によってゲームのソフトウェアをサーバから受信し、その受信したソフトウェアを用いて携帯電話機でゲームを楽しむことが可能である。

【0004】そして、ユーザは、自己の携帯電話機に受信したこのようなソフトウェアを他の携帯電話機へ送信したり、自己の記録媒体に格納するとき、自己の携帯電話機のメモリに格納されたソフトウェアを削除しなけれ

ばならない。

【0005】

【発明が解決しようとする課題】しかし、ユーザは、自己が使用して良かったので、そのソフトウェアを他人へプレゼントした場合、自己の携帯電話機に格納されたソフトウェアは削除されるので、そのプレゼントしたソフトウェアを、再度、使用することができないという問題がある。

【0006】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、取得したコンテンツデータを他の装置へ送信するときに削除しなければならぬコンテンツデータの流通を著作権を保護しながら促進するデータ端末装置を提供することである。

【0007】また、本発明の別の目的は、取得したコンテンツデータを他の装置へ送信するときに削除しなければならぬコンテンツデータの流通を著作権を保護しながら促進するデータ端末装置において実行されるプログラムを提供することである。

【0008】また、本発明のさらに別の目的は、取得したコンテンツデータを他の装置へ送信するときに削除しなければならぬコンテンツデータの流通を著作権を保護しながら促進するデータ端末装置において実行されるプログラムを記録した記録媒体を提供することである。

【0009】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、平文のコンテンツデータを取得してコンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵とを生成し、コンテンツデータの付加情報と、生成した暗号化コンテンツデータおよびライセンス鍵とをデータ記録装置との間で送受信するデータ端末装置であって、指示を入力するための操作部と、データ記録装置との間でデータをやり取りするインタフェースと、平文のコンテンツデータおよび付加情報を記憶する記憶手段と、ライセンス鍵を生成し、その生成したライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成する暗号化コンテンツ生成手段と、ライセンス鍵を含み、かつ、データ記録装置から前記ライセンス鍵が出力されたときデータ記録装置に記録されたライセンス鍵をデータ記録装置において実質的に削除するためのライセンスを生成するライセンス生成手段と、ライセンスを暗号化した暗号化ライセンスを生成する暗号処理手段と、制御手段とを備え、制御手段は、操作部を介して入力されたコンテンツデータのデータ記録装置への送信要求に応じて、平文のコンテンツデータおよび付加情報を記憶手段から読出し、その読出したコンテンツデータを暗号化コンテンツ生成手段に与え、暗号化コンテンツデータ、暗号化ライセンス、および付加情報をインタフェースを介してデータ記録装置へ送信し、記憶手段に記憶された平文のコンテンツデータを削

除し、付加情報は、コンテンツデータの取得元にアクセスするためのアクセス情報を少なくとも含む。

【0010】なお、本発明において、「実質的に削除」は、再生回数を「0」回に設定することによってデータ記録装置からのライセンス鍵の再出力を禁止すること、およびその他の方法を含む概念である。

【0011】したがって、この発明によれば、コンテンツデータのコピーを防止してコンテンツデータを流通させることができるとともに、データ記録装置に格納したコンテンツデータを容易に再取得できる。

【0012】好ましくは、記憶手段は、 $n$  ( $n$ は自然数) 個のコンテンツデータを記憶するデータ領域と、データ領域に記憶されているコンテンツデータに対応して、コンテンツデータの存在位置と、コンテンツデータの削除を示す  $m$  ( $m$ は  $m \geq n$  である自然数) 個のリスト情報とを記憶するリスト領域とを含み、制御手段は、コンテンツデータをデータ記録装置へ送信したとき、送信したコンテンツデータに対応するリスト情報を更新する。

【0013】したがって、この発明によれば、取得したコンテンツデータをデータ記録装置へ送信したとき、リスト情報を検索すれば、そのコンテンツデータの存在位置を容易に知ることができる。

【0014】好ましくは、制御手段は、操作部を介して入力されたコンテンツデータの再生要求に応じて、リスト領域に記憶されたリスト情報を読出し、その読出したリスト情報に基づいて再生要求されたコンテンツデータが記憶手段に記憶されているか否かを検索し、再生要求されたコンテンツデータが記憶手段に記憶されていないとき、付加情報に含まれるアクセス情報に基づいて再生要求されたコンテンツデータを再取得する。

【0015】したがって、この発明によれば、再生要求のあったコンテンツデータが記憶手段に存在しないとき、再生要求のあったコンテンツデータを再取得して容易に再生できる。

【0016】好ましくは、制御手段は、付加情報をコンテンツデータとともに取得し、その取得した付加情報をリスト領域に格納し、取得したコンテンツデータをデータ領域に格納する。

【0017】したがって、この発明によれば、コンテンツデータおよび付加情報を迅速に記憶手段に格納できる。

【0018】好ましくは、制御手段は、コンテンツデータを取得すると、その取得したコンテンツデータの付加情報を作成し、その作成した付加情報をリスト領域に格納する。

【0019】したがって、この発明によれば、コンテンツデータを受信した端末装置が独自の付加情報を作成できる。

【0020】好ましくは、ライセンス生成手段は、暗号

化コンテンツデータを復号および再生する回数を1回に設定した再生条件と、ライセンス鍵とからライセンスを生成する。

【0021】データ記録装置に格納されたコンテンツデータを再生するとき、そのコンテンツデータはデータ記録装置から外部へ出力され、再生回数が0回に設定される。

【0022】したがって、この発明によれば、再生回数を1回に制限することによってデータ記録装置におけるコンテンツデータの削除を容易に行なうことができる。

【0023】好ましくは、暗号化コンテンツ生成手段は、ライセンス鍵を生成する鍵生成部と、ライセンス鍵によってコンテンツデータを暗号化する暗号処理部とを含む。

【0024】データ端末装置において、コンテンツデータを暗号化するライセンス鍵が生成され、その生成されたライセンス鍵によってコンテンツデータが暗号化される。そして、暗号化コンテンツデータはデータ記録装置へ送信される。

【0025】したがって、この発明によれば、ローカルなライセンス鍵によってコンテンツデータを暗号化し、データ記録装置との間で暗号化コンテンツデータの送受信を行なうことができる。

【0026】好ましくは、暗号処理手段は、データ記録装置から受信した第2のセッション鍵によってライセンスを暗号化する。

【0027】ライセンスは、データ記録装置において生成された第2のセッション鍵によって暗号化されてデータ記録装置へ送信される。

【0028】したがって、この発明によれば、コンテンツデータをデータ記録装置へ送信するとき、データが漏洩し難い。

【0029】好ましくは、データ端末装置は、データ記録装置との通信を特定するための第1のセッション鍵を生成するセッション鍵生成手段と、第1のセッション鍵によって暗号化されたデータを復号する復号処理手段とをさらに備え、ライセンスのデータ記録装置への送信時、セッション鍵生成手段は、ライセンスのデータ記録装置への送信を特定する第1のセッション鍵を生成し、制御手段は、第1のセッション鍵をインタフェースを介してデータ記録装置へ送信し、第1のセッション鍵によって暗号化された第2のセッション鍵をインタフェースを介してデータ記録装置から受取り、その受取った第1のセッション鍵によって暗号化された第2のセッション鍵を復号処理手段に与える。

【0030】コンテンツデータをデータ記録装置へ送信するとき、データ記録装置との間でセッション鍵のやり取りが行なわれる。そして、データ端末装置は、自己が生成した第1のセッション鍵によって暗号化された、データ記録装置において生成された第2のセッション鍵を

データ記録装置から受信する。

【0031】したがって、この発明によれば、データ端末装置は、コンテンツデータをデータ記録装置へ送信する途中においても相互認証を行ないながらコンテンツデータを送信できる。

【0032】好ましくは、データ端末装置は、データ記録装置との通信を特定するための第1のセッション鍵を生成するセッション鍵生成手段と、第1のセッション鍵によって暗号化されたデータを復号する復号処理手段とをさらに備え、暗号処理手段は、データ記録装置に固有な第1の公開暗号鍵によってデータを暗号化する第1の暗号器と、データ記録装置において生成された第2のセッション鍵によってデータを暗号化する第2の暗号器とを含み、制御手段は、第1のセッション鍵によって暗号化された第2のセッション鍵と第1の公開暗号鍵とをデータ記録装置からインタフェースを介して受け、その受けた第1のセッション鍵によって暗号化された第2のセッション鍵と第1の公開暗号鍵とを復号処理手段に与え、復号処理手段によって復号された第1の公開暗号鍵を第1の暗号器に与え、復号処理手段によって復号された第2のセッション鍵を第2の暗号器に与え、第1の暗号器は、ライセンスを第1の公開暗号鍵によって暗号化し、第2の暗号器は、前記第1の暗号器の出力を第2のセッション鍵によって暗号化して暗号化ライセンスを生成する。

【0033】ライセンスをデータ記録装置へ送信するとき、ライセンスは、データ記録装置において保持された公開暗号鍵およびデータ記録装置において生成されたセッション鍵によって、順次、暗号化される。

【0034】したがって、この発明によれば、暗号化コンテンツデータを復号するためのライセンスを十分に保護してデータ記録装置へ送信できる。

【0035】好ましくは、データ端末装置は、第2の公開暗号鍵によってデータを暗号化するもう1つの暗号処理手段を備え、制御手段は、データ記録装置から第2の公開暗号鍵を含む認証データをインタフェースを介して受け、その受けた認証データが正当であると判断したとき、受けた認証データに含まれる第2の公開暗号鍵をもう1つの暗号処理手段に与え、もう1つの暗号処理手段において第2の公開暗号鍵によって暗号化された第1のセッション鍵をインタフェースを介してデータ記録装置へ送信し、もう1つの暗号処理手段は、セッション鍵生成手段によって生成された第1のセッション鍵を第2の公開暗号鍵によって暗号化する。

【0036】データ端末装置は、自己が生成したセッション鍵をデータ記録装置へ送信するとき、データ記録装置から認証データを認証した上で、自己が生成したセッション鍵を認証データに含まれる公開暗号鍵によって暗号化してデータ記録装置へ送信する。

【0037】したがって、この発明によれば、不正な相

手へのデータの送信を防止できる。好ましくは、データ端末装置は、データ記録装置に対する認証データを保持する認証データ保持部をさらに備え、制御手段は、操作部から入力された暗号化コンテンツデータのデータ記録装置からの受信要求に応じて、認証データをインタフェースを介してデータ記録装置へ送信し、認証データがデータ記録装置において認証されると、データ記録装置から暗号化コンテンツデータおよびライセンス鍵をインタフェースを介して受信する。

【0038】データ記録装置からコンテンツデータを受信するとき、データ記録装置に対するデータ端末装置の正当性が確認されたとき、データ端末装置は、暗号化コンテンツデータおよびライセンス鍵を受信する。

【0039】したがって、この発明によれば、データ記録装置からのコンテンツデータの不正なデータ端末装置への出力を防止できる。

【0040】好ましくは、制御手段は、データ記録装置においてライセンス鍵を実質的に削除するための処理が行なわれると、暗号化コンテンツデータおよびライセンス鍵をインタフェースを介して受信する。

【0041】データ記録装置からコンテンツデータがデータ端末装置へ送信されるとき、データ記録装置に記録されたコンテンツデータは削除される。

【0042】したがって、この発明によれば、コンテンツデータを取得したデータ端末装置へコンテンツデータを返却するときにもコンテンツデータのコピーを禁止できる。

【0043】好ましくは、データ端末装置は、暗号化コンテンツデータをライセンス鍵によって復号する復号処理手段をさらに備え、制御手段は、暗号化コンテンツデータおよびライセンス鍵を復号処理手段に与え、復号処理手段によって復号されたコンテンツデータを記憶手段に格納する。

【0044】データ端末装置は、データ記録装置から暗号化コンテンツデータおよびライセンス鍵を受信すると、ライセンス鍵によって暗号化コンテンツデータを復号し、その復号した平文のコンテンツデータを記憶手段に格納する。

【0045】したがって、この発明によれば、データ記録装置からデータ端末装置へのコンテンツデータの送信においてもコンテンツデータを保護できる。

【0046】好ましくは、データ端末装置は、データ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成手段と、セッション鍵生成手段が生成したセッション鍵によって暗号化されたデータを復号するもう一つの復号処理手段とをさらに備え、コンテンツデータのデータ記録装置からの受信時、セッション鍵生成手段は、コンテンツデータのデータ記録装置からの受信を特定するセッション鍵を生成し、制御手段は、セッション鍵をインタフェースを介してデータ記録装置へ

送信し、セッション鍵によって暗号化されたライセンス鍵をインタフェースを介してデータ記録装置から受取り、その受取ったセッション鍵によって暗号化されたライセンス鍵をもう一つの復号処理手段に与える。

【0047】コンテンツデータをデータ記録装置から受信するとき、データ端末装置は、データ記録装置との間でセッション鍵のやり取りを行ない、自己が生成したセッション鍵によって暗号化されたライセンス鍵をデータ記録装置から受信する。

10 【0048】したがって、この発明によれば、データ端末装置は、コンテンツデータをデータ記録装置から受信する途中においても相互認証を行ないながらコンテンツデータを受信できる。

【0049】好ましくは、コンテンツデータは、平文で実行可能なデータもしくはプログラムである。

【0050】各種のデータおよびプログラムがデータ端末装置とデータ記録装置との間でやり取りされる。

20 【0051】したがって、この発明によれば、データおよびプログラムのコピーを禁止してデータおよびプログラムを流通させることができる。

【0052】また、この発明によるデータ端末装置は、コンテンツデータとコンテンツデータを再び取得するために必要な取得情報とを外部から取得して格納し、コンテンツデータを利用するデータ端末装置であって、指示を入力するための操作手段と、コンテンツデータおよび取得情報を記憶する記憶手段と、制御手段とを備え、制御手段は、操作手段からの指示に従って、記憶手段に記憶されたコンテンツデータを削除するとき、その削除するコンテンツデータに対応した取得情報を保持するように記憶手段を制御し、削除したコンテンツデータを利用するように操作手段から指示されたとき、記憶手段に格納されている取得情報に基づいて、削除したコンテンツデータを再び外部から取得して記憶手段に格納する。

30 【0053】この発明によるデータ端末装置においては、外部から取得したコンテンツデータを削除しても、その削除したコンテンツデータを再取得するための取得情報はデータ端末装置に保持される。

【0054】したがって、この発明によれば、削除したコンテンツデータを再利用できる。好ましくは、記憶手段は、記憶している、または記憶していた複数のコンテンツデータの記憶状態と識別情報とを含むコンテンツリストをさらに記憶し、制御手段は、操作手段からの指示に従ってコンテンツデータおよび取得情報を新たに取得したとき、新たに取得したコンテンツデータおよび取得情報を記憶手段に格納し、かつ、コンテンツリストに新たに取得したコンテンツデータに対応した記憶状態と識別情報とを追加し、操作手段からの指示に従って記憶手段に記憶されたコンテンツデータを削除するとき、削除するコンテンツデータが記憶手段に格納されていないことを確認できるように、削除するコンテンツデータに対

応する記憶状態を変更し、削除したコンテンツデータを外部から再取得したとき、再取得したコンテンツデータが記憶手段に格納されていることを確認できるように、再取得したコンテンツデータに対応する記憶状態を変更し、操作手段からコンテンツデータの利用を指示されたとき、コンテンツリストに基づいて、指示されたコンテンツデータが記憶手段に格納されているか否かを確認する。

【0055】コンテンツデータの新規取得、削除、およびおよび再取得に応じて、対象となるコンテンツデータの記憶手段における記憶状態を更新し、コンテンツデータの利用指示があったとき、更新した記憶状態を参照して対象となるコンテンツデータを確認する。

【0056】したがって、この発明によれば、各種の動作要求に対して迅速に処理を行なうことができる。

【0057】好ましくは、コンテンツリストは、取得情報をさらに含み、制御手段は、コンテンツデータを外部から新たに取得したとき、その取得したコンテンツデータに対応する取得情報も取得し、その取得した取得情報をコンテンツリストに格納する。

【0058】したがって、この発明によれば、コンテンツリストによってコンテンツデータを管理できる。

【0059】また、この発明によるプログラムは、平文のコンテンツデータを取得する第1のステップと、コンテンツデータの取得元へアクセスするためのアクセス情報を少なくとも含む付加情報と取得したコンテンツデータとを記憶手段に格納する第2のステップと、コンテンツデータを暗号化した暗号化コンテンツデータを復号するためのライセンス鍵を生成し、その生成したライセンス鍵によってコンテンツデータを暗号化した暗号化コンテンツデータを生成する第3のステップと、ライセンス鍵を含み、かつ、データ記録装置からライセンス鍵が出力されたときデータ記録装置に記録されたライセンス鍵をデータ記録装置において実質的に削除するためのライセンスを生成する第4のステップと、ライセンスを暗号化した暗号化ライセンスを生成する第5のステップと、暗号化コンテンツデータ、暗号化ライセンス、および付加情報をデータ記録装置へ送信する第6のステップと、記憶手段に記憶されたコンテンツデータを削除する第7のステップとをコンピュータに実行させるためのプログラムである。

【0060】したがって、この発明によれば、コンテンツデータのコピーを防止してコンテンツデータを流通させることができるとともに、データ記録装置に格納したコンテンツデータを容易に再取得できる。

【0061】好ましくは、第1のステップにおいて、コンテンツデータが取得されると付加情報が作成される。

【0062】したがって、この発明によれば、コンテンツデータを受信した端末装置において独自にコンテンツデータの付加情報を作成することができる。

【0063】好ましくは、付加情報は、第1のステップにおいてコンテンツデータとともに取得される。

【0064】したがって、この発明によれば、受信したコンテンツデータおよび付加情報を迅速に記憶手段に格納できる。

【0065】好ましくは、第1のステップにおいて、コンテンツデータが取得されるとコンテンツデータの存在位置を示すリスト情報がさらに作成され、第2のステップにおいて、作成されたリスト情報が記憶手段にさらに格納される。

【0066】したがって、この発明によれば、受信したコンテンツデータの存在位置をリスト情報に基づいて容易に知ることができる。

【0067】また、この発明による記録媒体は、請求項21から請求項24のいずれか1項に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0068】したがって、この発明によれば、著作権を保護しながらコンテンツデータの流通を図るプログラムを広く流通させることができる。

【0069】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0070】図1は、本発明によるデータ端末装置（携帯電話機）がコンテンツデータを取得する通信システムの全体構成を概念的に説明するための概略図である。

【0071】なお、コンテンツデータとは、画像データ（動画データを含む）、音声データ、およびゲームのプログラムなどの端末装置内のメモリに展開された状態で実行あるいは参照されるデータ全体を表す。以下においては、コンテンツデータとしてプログラムを代表例として説明する。

【0072】図1を参照して、配信サーバ10は、ユーザが自己の携帯電話機100を用いて送信したプログラムの配信要求をキャリア20を介して受取る。そして、配信サーバ10は、受取ったプログラムの配信要求に応じて、プログラムをキャリア20を介して携帯電話機100へ送信する。この場合、配信サーバ10は、平文のプログラムを携帯電話機100へ送信する。キャリア20は、携帯電話機100からのプログラムの配信要求を配信サーバ10へ送信し、配信サーバ10からのプログラムを携帯電話網により携帯電話機100へ送信する。

【0073】携帯電話機100は、携帯電話網を介してプログラムを受信し、その受信したプログラムを内蔵したメモリ（図示せず）に格納する。そして、携帯電話機100のユーザは、受信したプログラムを実行して各種の画像データを携帯電話機100の表示部に表示したり、表示部を見て各種のゲームを行なう。また、ユーザは、携帯電話機100のメモリに格納されたプログラム

15

を、自己のメモリカード 110 に格納したいとき、メモリカード 110 を携帯電話機 100 に装着し、メモリカード 110 へのプログラムの格納を携帯電話機 100 に指示する。

【0074】そして、プログラムをメモリカード 110 に格納するとき、携帯電話機 100 は、後述するように、ライセンス鍵を生成し、その生成したライセンス鍵によってメモリに格納されたプログラムを暗号化し、その暗号化したプログラムをライセンス鍵等のライセンスおよびプログラムの付加情報とともにメモリカード 110 に格納する。プログラムをメモリカード 110 に格納した後、携帯電話機 100 は、メモリに格納したプログラムを削除する。このとき、ライセンスには再生制限、すなわち、ライセンス鍵の出力制限を加えて格納する。具体的には、携帯電話機 100 は、メモリに格納されたプログラムを、再生回数を 1 回に限定してメモリカード 110 に格納する。詳細は後述する。

【0075】このように、携帯電話機 100 は、配信サーバ 10 から受信したプログラムを内蔵したメモリに格納し、その格納したプログラムを実行する。そして、携帯電話機 100 は、ユーザからの指示に応じて、プログラムをメモリカード 110 へ格納したとき、内蔵したメモリに格納されたプログラムを削除する。また、メモリカード 110 からプログラムを再生したとき、つまり、暗号化したプログラムと、ライセンス鍵を含むライセンスとをメモリカード 110 から取出したとき、それ以後、メモリカード 110 からライセンス鍵を取出すことはできない。すなわち、携帯電話機 100 は、プログラムをメモリカード 110 へ格納するとき、再生回数を 1 回に設定して格納するので、メモリカード 110 からプログラムを再生する、すなわち、メモリカード 110 からライセンス鍵を取出したとき、メモリカード 110 において再生回数が「0」回に設定され、それ以後、メモリカード 110 からライセンス鍵を取出すことはできない。したがって、メモリカード 110 から携帯電話機 100 へプログラムを取出したとき、メモリカード 110 には暗号化されたプログラムが格納されているが、ライセンス鍵が取出せなくなる。したがって、プログラムは携帯電話機 100 とメモリカード 110 の両方に利用可能な状態で格納されることはなく、必ず、一ヶ所に利用可能な状態で格納される。

【0076】また、メモリカード 110 は、携帯電話機 100 に脱着可能であり、携帯電話機 100 のユーザは、携帯電話機 100 のメモリに格納されたプログラムをメモリカード 110 に格納し、そのメモリカード 110 を介して他人にプレゼントすることができる。つまり、プログラムの自由なコピーを禁止してプログラムを流通することが可能となる。さらに、メモリカード 110 にプログラムを格納することによって、携帯電話機の機種を変更したときでも、変更後の携帯電話機にメモリ

16

カード 110 を装着し、メモリカード 110 からプログラムを読み出すことによって、変更後の携帯電話機においてプログラムを実行できる。

【0077】図 2 は、図 1 に示した通信システムにおいて、配信サーバ 10 と携帯電話機 100 との間、または携帯電話機 100 とメモリカード 110 との間で使用される通信のためのデータ、情報等の特性を説明する図である。

【0078】まず、配信サーバ 10 より配信されるデータについて説明する。Dc は、プログラムから成るコンテンツデータである。コンテンツデータ Dc は、平文の状態で配信サーバ 10 からキャリア 20 を介して携帯電話機 100 へ送信される。そして、コンテンツデータは、データ端末装置（携帯電話機）またはメモリカードに保持される。

【0079】また、コンテンツデータに付随する平文のデータとして付加情報 Dc-inf が存在する。図 3 を参照して、付加情報 Dc-inf は、購入関連の情報と、コンテンツ関連の情報と、購入者関連の情報とを含む。購入関連の情報は、ダウンロード先、ダウンロード先 2、ダウンロード先 3、購入金額、および時間から成る。ダウンロード先は、コンテンツデータをダウンロードする際のアクセス先、すなわち、配信サーバ 10 に接続するための URL、電話番号、およびコンテンツ ID 等のコンテンツを特定するまでの情報である。ダウンロード先 2 は、関連コンテンツ、付加エレメントのダウンロード先を表す情報である。ダウンロード先 3 は、コンテンツデータの次期バージョン、および体験バージョン等のダウンロード先を表す情報である。購入金額は、コンテンツデータを配信サーバ 10 から受信する際に支払う料金である。時間は、コンテンツデータのダウンロードに必要な時間である。

【0080】また、コンテンツ関連の情報は、コンテンツ名、コンテンツデータの作成者、コンテンツデータの再ダウンロード可能な有効期限、コンテンツデータのサイズ、およびコンテンツデータの種類から成る。

【0081】さらに、購入者関連の情報は、購入者情報、および購入日時から成る。購入者情報は、購入者名、およびダウンロード端末番号を表す。ダウンロード端末番号は、携帯電話機 100 を特定するための番号である。購入日時は、コンテンツデータをダウンロードした時間である。

【0082】本発明においては、携帯電話機 100 は、配信サーバ 10 からコンテンツデータを受信してメモリに格納するとき、図 3 に示す情報を含む付加情報をコンテンツデータとともにメモリに格納する。なお、付加情報 Dc-inf は、配信サーバ 10 からコンテンツデータとともに携帯電話機 100 へ配信される場合もあり、コンテンツデータが携帯電話機 100 へ配信されたとき、携帯電話機 100 において作成される場合もある。

【0083】再び、図2を参照して、ライセンスとして、暗号化されたコンテンツデータを復号するためのライセンス鍵Kcが存在する。ライセンス鍵Kcは、携帯電話機100に保持されたプログラムをメモリカード110へ送信するときに、携帯電話機100において生成される。そして、ライセンス鍵Kcは、ライセンス鍵Kcによって暗号化された暗号化コンテンツデータ{Dc}Kcとともに携帯電話機110とメモリカード110との間で送受信される。なお、以下においては、

{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0084】さらに、ライセンスとしては、記録装置(メモリカード)におけるライセンスのアクセスに対する制限に関する情報であるアクセス制限情報ACmが存在する。具体的には、アクセス制限情報ACmはメモリカードからライセンス鍵Kcを外部に出力するに当たっての制御情報であり、再生可能回数(再生のためにライセンス鍵を出力する数)がある。

【0085】さらに、ライセンスとして、暗号化コンテンツデータ{Dc}Kcを携帯電話機100からメモリカード110へ送信する際に、携帯電話機100のメモリに格納されたコンテンツデータを特定するための管理コードとしてのコンテンツIDが存在する。

【0086】さらに、ライセンスとして、暗号化コンテンツデータ{Dc}Kcを携帯電話機100からメモリカード110へ送信する際に生成されるライセンスを特定するための管理コードとしてのライセンスIDが存在する。

【0087】以後、ライセンス鍵Kcと、アクセス制限情報ACmと、コンテンツIDと、ライセンスIDとを併せて、ライセンスと総称することとする。

【0088】また、以降では、アクセス制限情報ACmは、再生回数の制限を行なう制御情報である再生回数(0:再生不可、1:再生可能回数)のみを制限するものとする。

【0089】図4は、図1に示す通信システムにおいて携帯電話機100とメモリカード110との間でプログラムが送受信される際に使用される認証のためのデータ、情報等の特性を説明する図である。

【0090】データ端末装置(携帯電話機)、およびメモリカードには固有の公開暗号鍵KpyおよびKpmwがそれぞれ設けられ、公開暗号鍵KpyおよびKpmwは、データ端末装置に固有の秘密復号鍵Kpyおよびメモリカードに固有の秘密復号鍵Kmwによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、データ端末装置、およびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造

会社や製品の種類、製造時のロット等によって異なる。

【0091】また、データ端末装置(携帯電話機)のクラス証明書としてCpyが設けられ、メモリカードのクラス証明書としてCmwが設けられる。これらのクラス証明書は、データ端末装置、およびメモリカードのクラスごとに異なる情報を有する。耐タンパモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、秘密復号鍵が漏洩したクラスに対しては、ライセンス取得の禁止対象となる。

【0092】これらのデータ端末装置のクラス公開暗号鍵およびクラス証明書は、認証データ{Kpy/Cpy}Kpaの形式で、メモリカードのクラス公開暗号鍵およびクラス証明書は認証データ{Kpmw/Cmw}Kpaの形式で、出荷時にデータ端末装置、およびメモリカードにそれぞれ記録される。後ほど詳細に説明するが、Kpaは配信システム全体で共通の公開認証鍵である。

【0093】また、メモリカード110内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵Kpmcxと、公開暗号鍵Kpmcxで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Kmcxが存在する。このメモリカードごとに個別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵Kpmcxを個別公開暗号鍵、秘密復号鍵Kmcxを個別秘密復号鍵と称する。

【0094】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、データ端末装置(携帯電話機)とメモリカードとの間でコンテンツデータの送受信が行なわれるごとに携帯電話機100、およびメモリカード110において生成される共通鍵Ks1~Ks4が用いられる。

【0095】ここで、共通鍵Ks1~Ks4は、データ端末装置とメモリカードとの間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ks1~Ks4を「セッション鍵」とも呼ぶこととする。

【0096】これらのセッション鍵Ks1~Ks4は、各セッションごとに固有の値を有することにより、データ端末装置、およびメモリカードによって管理される。具体的には、セッション鍵Ks1は、データ端末装置(携帯電話機)によってプログラムのメモリカードへの格納(ストアとも呼ぶ)ごとに発生される。セッション鍵Ks2は、メモリカードによってプログラムのメモリカードへのストアごとに発生され、セッション鍵Ks3は、プログラムの再生、すなわち、携帯電話機へのプログラムの格納(リストアとも呼ぶ)ごとにメモリカードによって発生され、セッション鍵Ks4は、携帯電話機へのプログラムのリストアごとに携帯電話機によって発生される。各セッションにおいて、これらのセッション

鍵を授受し、他の機器で生成されたセッション鍵を受け、このセッション鍵による暗号化を実行した上でコンテンツデータおよびライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0097】図5は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

【0098】携帯電話機100は、アンテナ1000と、送受信部1002と、マイク1004と、AD変換器1006と、音声符号化部1008と、音声再生部1010と、DA変換部1012と、スピーカ1016と、キー操作部1018と、ディスプレイ1020と、コントローラ1022と、ROM1023と、メモリ1024と、メモリカードインタフェース1026と、復号処理部1028、1036、1044、1048と、認証鍵保持部1030と、乱数鍵発生部1032と、暗号処理部1034、1038、1040、1042と、Kp保持部1046と、スイッチ1050、1052と、認証データ保持部1500とを備える。

【0099】アンテナ1000は、携帯電話網により無線伝送される信号を受信する。送受信部1002は、アンテナ1000からの信号を受けてベースバンド信号に変換、あるいは携帯電話機100からのデータを変調してアンテナ1000に与える。バスBS1は、携帯電話機100の各部のデータ授受を行なう。マイク1004は、携帯電話機100のユーザの音声データを取込み、音声データをAD変換器1006へ出力する。AD変換器1006は、音声データをアナログ信号からデジタル信号に変換する。音声符号化部1008は、デジタル信号に変換された音声信号を所定の方式に符号化する。音声再生部1010は、他の携帯電話機から受信した音声信号を復号する。DA変換器1012は、音声再生部1010からの音声信号をデジタル信号からアナログ信号に変換して音声データを出力する。スピーカ1016は、音声データを外部へ出力する。

【0100】キー操作部1018は、外部からの指示を携帯電話機100に与える。ディスプレイ1020は、コントローラ1022等から出力される情報をユーザに視覚情報として与える。また、コントローラ1022は、バスBS1を介してROM1023に格納された動作プログラムを読み出し、その読み出した動作プログラムに従って後述する各種の動作を行なう。ROM1023は、コントローラ1022において実行される動作プログラムを格納する。メモリ1024は、配信サーバ10から受信したコンテンツデータとしてのプログラムと、付加情報Dc-infと、リスト情報LSTとを格納する。リスト情報LSTは、メモリ1024上に格納されたプログラムおよびメモリカード110へストアしたプログラムごとにコンテンツID、コンテンツデータDc、および付加情報Dc-infの格納位置、格納日時

(携帯電話機へのダウンロード日時)等から成る。メモリカード110へストアされた場合、コンテンツデータDcの格納位置が更新され、ストアしたことを示すように設定される。リスト情報LSTは、携帯電話機100において生成され、全てのコンテンツデータDcに対するリスト情報LSTは、1つのコンテンツリストCLSTを構成する。メモリカードインタフェース1026は、メモリカード110とバスBS1との間のデータの授受を制御する。

【0101】復号処理部1028は、プログラムを携帯電話機100からメモリカード110へ格納するセッションにおいて、メモリカード110から受信した認証データを認証鍵保持部1030からの公開認証鍵KPaによって復号する。認証鍵保持部1030は、公開認証鍵KPaを保持する。乱数鍵発生部1032は、プログラムのメモリカード110へのストア時、またはプログラムをメモリカード110から携帯電話機100へ格納するセッションにおいてセッション鍵Ks1、Ks4およびライセンス鍵Kcを発生する。

【0102】暗号処理部1034は、プログラムのストア時に、乱数鍵発生部1032によって発生されたセッション鍵Ks1を、復号処理部1028によって復号して得られた公開暗号鍵Kpmwによって暗号化し、その結果をバスBS1へ出力する。復号処理部1036は、プログラムのストア時に、セッション鍵Ks1によって暗号化された暗号化データをメモリカード110からバスBS1を介して受け、その受けた暗号化データをセッション鍵Ks1によって復号する。

【0103】暗号処理部1038は、メモリ1024に格納されたプログラムDcをバスBS1を介して受け、その受けたプログラムDcを、乱数鍵発生部1032によって発生されたライセンス鍵Kcによって暗号化して暗号化プログラム{Dc}KcをバスBS1へ出力する。暗号処理部1040は、プログラムのストア時に、乱数鍵発生部1032によって発生されたライセンス鍵Kc、ライセンスを特定するための管理コードであるライセンスID、およびアクセス制限情報ACmを公開暗号鍵Kpmcwによって暗号化し、暗号化データ{ライセンスID//Kc//ACm}Kmcwをスイッチ1050の端子Pbへ出力する。

【0104】暗号処理部1042は、プログラムのストア時、スイッチ1050の端子Pa、Pbを、順次、切換えることによって得られる暗号化データ{ライセンスID//Kc//ACm}Kmcwをセッション鍵Ks2によって暗号化し、暗号化データ{ライセンスID//Kc//ACm}Kmcw}Ks2をバスBS1へ出力する。

【0105】復号処理部1044は、プログラムのリストア時に、公開暗号鍵Kppによって暗号化された暗号化データをメモリカード110からバスBS1を介して

受け、その受けた暗号化データを秘密復号鍵K<sub>p</sub>によって復号する。K<sub>p</sub>保持部1046は、クラス固有の秘密復号鍵K<sub>p</sub>を保持する。復号処理部1048は、プログラムのリストア時、暗号化コンテンツデータ{D<sub>c</sub>}K<sub>c</sub>をメモ리카ード110からバスBS1を介して受け、その受けた暗号化コンテンツデータ{D<sub>c</sub>}K<sub>c</sub>を、乱数鍵発生部1032によって発生されたライセンス鍵K<sub>c</sub>によって復号し、コンテンツデータをバスBS1へ出力する。認証データ保持部1500は、クラス公開暗号鍵K<sub>Pp1</sub>およびクラス証明書C<sub>p1</sub>を公開認証鍵K<sub>Pa</sub>で復号することでその正当性を認証できる状態に暗号化した認証データ{K<sub>Pp1</sub>/C<sub>p1</sub>}K<sub>Pa</sub>を保持する。ここで、携帯電話機100のクラスyは、y=1であるとする。

【0106】携帯電話機100の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0107】図6は、図1に示すメモ리카ード110の構成を説明するための概略ブロック図である。図6を参照して、メモ리카ード110は、認証データ保持部1400と、K<sub>mc</sub>保持部1402と、復号処理部1404、1408、1412、1422と、暗号処理部1406、1410と、認証鍵保持部1414と、メモリ1415と、K<sub>Pmc</sub>保持部1416と、乱数鍵発生部1418と、コントローラ1420と、K<sub>m</sub>保持部1421と、インタフェース1424と、端子1426と、スイッチ1442、1446とを備える。

【0108】すでに説明したように、メモ리카ードのクラス公開暗号鍵およびクラス秘密復号鍵として、K<sub>Pmw</sub>およびK<sub>m</sub>wが設けられ、メモ리카ードのクラス証明書C<sub>mw</sub>が設けられるが、メモ리카ード110においては、自然数w=5で表わされるものとする。また、メモ리카ードを識別する自然数xはx=6で表されるものとする。

【0109】したがって、認証データ保持部1400は、認証データ{K<sub>Pm5</sub>/C<sub>m5</sub>}K<sub>Pa</sub>を保持する。バスBS2は、メモ리카ード110の各部のデータ授受を行なう。K<sub>mc</sub>保持部1402は、メモ리카ードごとに設定される固有の復号鍵である個別秘密復号鍵K<sub>mc6</sub>を保持する。復号処理部1404は、バスBS2上のデータを個別公開暗号鍵K<sub>Pmc6</sub>と対をなすメモ리카ード110の個別秘密復号鍵K<sub>mc6</sub>によって復号する。

【0110】暗号処理部1406は、スイッチ1442によって選択的に与えられる鍵によって、スイッチ1446によって選択的に与えられるデータを暗号化してバスBS2に出力する。復号処理部1408は、認証鍵保持部1414から公開認証鍵K<sub>Pa</sub>を受けて、バスBS2に与えられるデータから公開認証鍵K<sub>Pa</sub>による復号処理を実行して復号結果と得られたクラス証明書をコン

トローラ1420に、得られたクラス公開鍵を暗号処理部1410に出力する。暗号処理部1410は、乱数鍵発生部1418が出力したセッション鍵K<sub>s3</sub>を復号処理部1408によって得られるクラス公開暗号鍵K<sub>Ppy</sub>によって暗号化してバスBS2に出力する。

【0111】復号処理部1412は、バスBS2よりセッション鍵K<sub>s2</sub>によって暗号化されたデータを受け、その受けたデータを乱数鍵発生部1418により発生されたセッション鍵K<sub>s2</sub>によって復号する。認証鍵保持部1414は、公開認証鍵K<sub>Pa</sub>を保持する。K<sub>Pmc</sub>保持部1416は、個別秘密復号鍵K<sub>mc6</sub>によって復号可能な公開暗号鍵K<sub>Pmc6</sub>を保持する。乱数鍵発生部1418は、プログラムのストア時、またはリストア時の各セッションにおいてセッション鍵K<sub>s2</sub>、K<sub>s3</sub>を発生する。

【0112】メモリ1415は、暗号化コンテンツデータ{D<sub>c</sub>}K<sub>c</sub>と、暗号化コンテンツデータ{D<sub>c</sub>}K<sub>c</sub>を再生するためのライセンス(K<sub>c</sub>、AC<sub>m</sub>、ライセンスID)とをバスBS2より受けて格納する。メモリ1415は、例えば半導体メモリによって構成される。また、メモリ1515は、ライセンス領域1415Aと、データ領域1415Bとから成る。ライセンス領域1415Aは、ライセンスを記録するための領域である。データ領域1415Bは、暗号化コンテンツデータ{D<sub>c</sub>}K<sub>c</sub>、ライセンスを管理するために必要な情報であるライセンス管理情報を暗号化コンテンツごとに記録するライセンス管理ファイル、およびメモ리카ードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リストファイルを記録するための領域である。そして、データ領域1415Bは、外部から、直接、アクセスすることが可能である。ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【0113】ライセンス領域1415Aは、ライセンス(ライセンス鍵K<sub>c</sub>、アクセス制限情報AC<sub>m</sub>、ライセンスID)を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスを格納する。ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【0114】なお、データ領域1415Bを除く全ての構成は、耐タンパモジュール領域に構成される。

【0115】コントローラ1420は、バスBS2を介して外部との間でデータ授受を行ない、バスBS2との間で各種の情報等を受けて、メモ리카ード110の動作を制御する。K<sub>m</sub>保持部1421は、クラス秘密復号鍵K<sub>m5</sub>を保持する。インタフェース1424は、メモリインタフェース1026との間で信号を端子1426を介して授受する。復号処理部1422は、バスBS2にインタフェース1424から与えられるデータを、K<sub>m</sub>

保持部 1421 から受けたクラス秘密復号鍵  $K_{m5}$  によって復号し、携帯電話機 100 がプログラムのストア時において生成したセッション鍵  $K_{s1}$  を接点  $P_a$  に出力する。

【0116】 上述したように、メモリカードという記録装置の暗号鍵を設けることによって、携帯電話機 100 から格納されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0117】 以下、図 1 に示す通信システムにおける各セッションの動作について説明する。

【0118】 [プログラムの購入] まず、図 1 に示す通信システムにおいて、携帯電話機 100 のユーザが配信サーバ 10 からコンテンツデータを購入する動作について説明する。

【0119】 図 7 は、コンテンツデータを配信サーバ 10 から携帯電話機 100 へ受信する動作を説明するためのフローチャートである。

【0120】 図 7 を参照して、携帯電話機 100 のキー操作部 1018 を介してコンテンツデータの購入要求が入力されると (ステップ S10) と、コントローラ 1022 は、バス  $BS1$  を介してコンテンツデータの購入要求を受け、送受信部 1002 およびアンテナ 1000 を介して配信サーバ 10 へ発呼し、回線を接続する (ステップ S20)。配信サーバ 10 は、携帯電話機 100 からコンテンツデータの購入要求を受信すると、自己が保持するコンテンツデータのリストを携帯電話機 100 へ送信する。そして、携帯電話機 100 のコントローラ 1022 は、アンテナ 1000 および送受信部 1002 を介してコンテンツデータのリストを受信し、その受信したリストをバス  $BS1$  を介してディスプレイ 1020 に表示する。携帯電話機 100 のユーザがディスプレイ 1020 に表示されたコンテンツデータのリストを見て、購入したいコンテンツデータを特定するためのコンテンツ ID をキー操作部 1018 から入力すると、コントローラ 1022 は、バス  $BS1$  を介してコンテンツ ID を受取り、その受取ったコンテンツ ID を送受信部 1002 およびアンテナ 1000 を介して配信サーバ 10 へ送信する。

【0121】 そうすると、配信サーバ 10 は、受信したコンテンツ ID に基づいてコンテンツデータを検索し (ステップ S30)、コンテンツ ID によって特定されたコンテンツデータ  $D_c$  を抽出する。そして、配信サーバ 10 は、抽出したコンテンツデータ  $D_c$  を携帯電話機 100 へ送信し、コンテンツデータ  $D_c$  のダウンロードが開始される (ステップ S40)。この場合、コンテンツデータ  $D_c$  の付加情報  $D_{c-inf}$  も携帯電話機 100 へ配信される。

【0122】 コンテンツデータ  $D_c$  および付加情報  $D_{c-inf}$  が携帯電話機 100 へ配信されると、コンテン

ツデータ  $D_c$  の書き込み要求が発生し (ステップ S50)、コントローラ 1022 は、アンテナ 1000 および送受信部 1002 を介して受信したコンテンツデータ  $D_c$  をバス  $BS1$  を介してメモリ 1024 に書き込む (ステップ S60)。そして、コントローラ 1022 は、コンテンツデータ  $D_c$  の存在位置やコンテンツデータ  $D_c$  を受信した日時等から成るリスト情報  $LST$  を作成し (ステップ S70)、その作成したリスト情報  $LST$  をメモリ 1024 に格納されているコンテンツリスト  $CLST$  に登録し、バス  $BS1$  を介してメモリ 1024 に書き込む。ここで、リスト情報  $LST$  のコンテンツリスト  $CLST$  上の登録位置はユーザが選択してもよい。また、コントローラ 1022 は、コンテンツデータ  $D_c$  とともに受信した付加情報  $D_{c-inf}$  をメモリ 1024 に書き込む (ステップ S80)。そして、コンテンツデータ  $D_c$  の購入動作が終了する (ステップ S90)。

【0123】 なお、上記においては、コンテンツデータ  $D_c$  の付加情報  $D_{c-inf}$  は、コンテンツデータ  $D_c$  とともに配信サーバ 10 から携帯電話機 100 へ配信されるとして説明したが、本発明においては、付加情報  $D_{c-inf}$  は、コンテンツデータ  $D_c$  を受信した携帯電話機 100 において作成されてもよい。この場合、携帯電話機 100 のコントローラ 1022 は、配信サーバ 10 への発呼からコンテンツデータ  $D_c$  の受信までの動作に基づいて付加情報  $D_{c-inf}$  を作成する。そして、コントローラ 1022 は、作成した付加情報  $D_{c-inf}$  をメモリ 1024 に格納する。

【0124】 [プログラムのストア] 次に、携帯電話機 100 が配信サーバ 10 から受信し、かつ、メモリ 1024 に格納したコンテンツデータ  $D_c$  をメモリカード 110 に格納する動作について説明する。なお、コンテンツデータが携帯電話機 100 からメモリカード 110 へ格納される動作を「ストア」という。

【0125】 図 8 および図 9 は、図 1 に示す通信システムにおける携帯電話機 100 からメモリカード 110 へのプログラムのストアの動作を説明するための第 1 および第 2 のフローチャートである。

【0126】 図 8 を参照して、携帯電話機 100 のユーザからキー操作部 1018 を介してコンテンツデータを指定したストア要求がなされる (ステップ S100)。

【0127】 コンテンツデータのストア要求が入力されると、コントローラ 1022 は、バス  $BS1$  およびメモリカードインタフェース 1026 を介してメモリカード 110 へ認証データの送信要求を送信する (ステップ S102)。メモリカード 110 のコントローラ 1420 は、端子 1426、インタフェース 1424 およびバス  $BS2$  を介して認証データの送信要求を受信する (ステップ S104)。そして、コントローラ 1420 は、バス  $BS2$  を介して認証データ保持部 1400 から認証データ  $\{K_{Pm5}/C_{m5}\} K_{Pa}$  を読出し、認証デー

25

タ {K P m 5 / / C m 5} K P a をバス B S 2、インタフェース 1 4 2 4 および端子 1 4 2 6 を介して出力する (ステップ S 1 0 6)。

【0128】携帯電話機 100 のコントローラ 1022 は、メモ리카ード 110 からの認証データ {K P m 5 / / C m 5} K P a をメモ리카ードインタフェース 1026 およびバス B S 1 を介して受取り (ステップ S 108)、その受取った認証データ {K P m 5 / / C m 5} K P a を復号処理部 1028 に与える。復号処理部 1028 は、認証データ {K P m 5 / / C m 5} K P a を、認証鍵保持部 1030 からの公開認証鍵 K P a によって復号する (ステップ S 110)。コントローラ 1022 は、復号処理部 1028 における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう (ステップ S 112)。正当な認証データであると判断された場合、コントローラ 1022 は、クラス公開暗号鍵 K P m 5 およびクラス証明書 C m 5 を承認し、受理する。そして、次の処理 (ステップ S 114) へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵 K P m 5 およびクラス証明書 C m 5 を受理しないでストアの動作を終了する (ステップ S 162)。

【0129】認証の結果、プログラムを格納するメモ리카ード 110 が正当な認証データを持つメモ리카ードであることが確認されると、乱数鍵発生部 1032 は、プログラムのストアのためのセッション鍵 K s 1 を生成する (ステップ S 114)。そして、暗号処理部 1034 は、乱数鍵発生部 1032 からのセッション鍵 K s 1 を、復号処理部 1028 からの公開暗号鍵 K P m 5 によって暗号化し、暗号化データ {K s 1} K m 5 をバス B S 1 に出力する。コントローラ 1022 は、ライセンス ID を生成し (ステップ S 118)、その生成したライセンス ID と暗号処理部 1034 からの暗号化データ {K s 1} K m 5 とを 1 つのデータにしてライセンス ID / / {K s 1} K m 5 をバス B S 1 およびメモ리카ードインタフェース 1026 を介してメモ리카ード 110 へ送信する (ステップ S 120)。

【0130】メモ리카ード 110 のコントローラ 1420 は、端子 1426、インタフェース 1424、およびバス B S 2 を介してライセンス ID / / {K s 1} K m 5 を受信し (ステップ S 122)、その受信した暗号化データ {K s 1} K m 5 をバス B S 2 を介して復号処理部 1422 に与える。復号処理部 1422 は、暗号化データ {K s 1} K m 5 を、K m 保持部 1421 からの秘密復号鍵 K m 5 によって復号し、携帯電話機 100 において生成されたセッション鍵 K s 1 を受理する (ステップ S 124)。

【0131】そうすると、コントローラ 1420 は、乱数鍵発生部 1418 を制御し、乱数鍵発生部 1418

26

は、セッション鍵 K s 2 を生成する (ステップ S 126)。暗号処理部 1406 は、スイッチ 1446 の接点 P c、P d を順次切換えることによって受取ったセッション鍵 K s 2 と公開暗号鍵 K P m c 6 とを、スイッチ 1442 の接点 P a を介して受取ったセッション鍵 K s 1 によって暗号化し、暗号化データ {K s 2 / / K P m c 6} K s 1 をバス B S 2 へ出力する。そして、コントローラ 1420 は、暗号化データ {K s 2 / / K P m c 6} K s 1 をバス B S 2、インタフェース 1424、および端子 1426 を介して携帯電話機 100 へ送信する (ステップ S 128)。

【0132】携帯電話機 100 のコントローラ 1022 は、メモ리카ードインタフェース 1026 およびバス B S 1 を介して暗号化データ {K s 2 / / K P m c 6} K s 1 を受取り (ステップ S 130)、その受取った暗号化データ {K s 2 / / K P m c 6} K s 1 をバス B S 1 を介して復号処理部 1036 に与える。復号処理部 1036 は、暗号化データ {K s 2 / / K P m c 6} K s 1 を、乱数鍵発生部 1032 によって発生されたセッション鍵 K s 1 によって復号してセッション鍵 K s 2 および公開暗号鍵 K P m c 6 を受理する (ステップ S 132)。

【0133】コントローラ 1022 は、メモ리카ード 110 において発生されたセッション鍵 K s 2 およびメモ리카ード 110 に固有の公開暗号鍵 K P m c 6 の受理を確認すると、ライセンス鍵 K c を発生するように乱数鍵発生部 1032 を制御し、乱数鍵発生部 1032 はライセンス鍵を生成する (ステップ S 134)。そして、コントローラ 1022 は、再生回数を 1 回に限定したアクセス制限情報 A C m を設定する (ステップ S 136)。その後、コントローラ 1022 は、バス B S 1 を介してメモリ 1024 からコンテンツデータ D c を読出し、その読出したコンテンツデータ D c をバス B S 1 を介して暗号処理部 1038 に与える。暗号処理部 1038 は、バス B S 1 を介して受取ったコンテンツデータ D c を、乱数鍵発生部 1032 からのライセンス鍵 K c によって暗号化して暗号化コンテンツデータ {D c} K c をバス B S 1 へ出力する (ステップ S 138)。そして、コントローラ 1022 は、バス B S 1 を介してメモリ 1024 から付加情報 D c - i n f を読出し、その読出した付加情報 D c - i n f と、暗号処理部 1038 からバス B S 1 に出力された暗号化コンテンツデータ {D c} K c とをメモ리카ードインタフェース 1026 を介してメモ리카ード 110 へ送信する (ステップ S 140)。

【0134】メモ리카ード 110 のコントローラ 1420 は、端子 1426、インタフェース 1424、およびバス B S 2 を介して暗号化コンテンツデータ {D c} K c および付加情報 D c - i n f を受取り、その受取った暗号化コンテンツデータ {D c} K c および付加情報 D c - i n f をバス B S 2 を介してメモリ 1415 のデー

27

タ領域 1415B に格納する (ステップ S142)。

【0135】そうすると、携帯電話機 100 のコントローラ 1022 は、バス BS1 を介してメモリ 1024 に格納されたコンテンツデータを削除する (ステップ S144)。

【0136】図 9 を参照して、コントローラ 1022 は、ライセンス ID、およびアクセス制限情報 ACm をバス BS1 を介して暗号処理部 1040 に与える。暗号処理部 1040 は、バス BS1 を介して受取ったライセンス ID およびアクセス制限情報 ACm と、乱数鍵発生部 1032 からのライセンス鍵 Kc とを、復号処理部 1036 からの公開暗号鍵 Kpmc6 によって暗号化し、暗号化データ {ライセンス ID // Kc // ACm} Kmc6 をスイッチ 1050 の接点 Pb へ出力する (ステップ S146)。そうすると、暗号処理部 1042 は、スイッチ 1050 の接点 Pb を介して受取った暗号化データ {ライセンス ID // Kc // ACm} Kmc6 を、スイッチ 1052 の接点 Pc を介して受取ったセッション鍵 Ks2 によって暗号化し、暗号化データ { {ライセンス ID // Kc // ACm} Kmc6 } Ks2 をバス BS1 へ出力する (ステップ S148)。そして、コントローラ 1022 は、バス BS1 上の暗号化データ { {ライセンス ID // Kc // ACm} Kmc6 } Ks2 をメモ리카ードインタフェース 1026 を介してメモ리카ード 110 へ送信する (ステップ S150)。

【0137】メモ리카ード 110 のコントローラ 1420 は、端子 1426、インタフェース 1424、およびバス BS2 を介して暗号化データ { {ライセンス ID // Kc // ACm} Kmc6 } Ks2 を受信する (ステップ S152)。コントローラ 1420 は、暗号化データ { {ライセンス ID // Kc // ACm} Kmc6 } Ks2 をバス BS2 を介して復号処理部 1412 に与える。復号処理部 1412 は、暗号化データ { {ライセンス ID // Kc // ACm} Kmc6 } Ks2 をセッション鍵 Ks2 によって復号し、暗号化データ {ライセンス ID // Kc // ACm} Kmc6 を受取する (ステップ S154)。復号処理部 1404 は、復号処理部 1412 によって復号された暗号化データ {ライセンス ID // Kc // ACm} Kmc6 を、Kmc6 保持部 1402 からの秘密復号鍵 Kmc6 によって復号し、ライセンス ID、ライセンス鍵 Kc、およびアクセス制限情報 ACm を受取する (ステップ S156)。

【0138】そうすると、携帯電話機 100 のコントローラ 1022 は、ライセンスを格納するためのエントリ番号を決定し、その決定したエントリ番号とライセンスの格納要求とをバス BS1 およびメモ리카ードインタフェース 1026 を介してメモ리카ード 110 へ送信する (ステップ S158)。

【0139】メモ리카ード 110 のコントローラ 1420 は、端子 1426、インタフェース 1424、および

28

バス BS2 を介してエントリ番号および格納要求を受信し、バス BS2 を介して、ライセンス ID、ライセンス鍵 Kc、およびアクセス制限情報 ACm を、メモリ 1415 のライセンス領域 1415A の指示されたエントリに格納する (ステップ S159)。そして、携帯電話機 100 のコントローラ 1022 は、生成したライセンス鍵 Kc を破棄し (ステップ S160)、メモリ 1024 に格納されたリスト情報 LST にストアされたこと記録してリスト情報を更新し (ステップ S161)、プログラムのメモ리카ード 110 へのストアの動作が終了する (ステップ S162)。

【0140】このように、携帯電話機 100 が配信サーバ 10 から受信し、メモリ 1024 に格納したコンテンツデータ Dc としてのプログラムをメモ리카ード 110 へストアするとき、メモ리카ード 110 が正規のメモ리카ードであるか否かを判定し、正規のメモ리카ードであることが確認されたときに (図 8 のステップ S112 参照)、コンテンツデータ Dc がメモ리카ード 110 へ送信される (図 8 のステップ S140 参照)。したがって、コンテンツデータ Dc としてのプログラムは、不正なメモ리카ードに格納されることはなく、十分に保護される。

【0141】また、プログラムをメモ리카ード 110 へストアするとき、コンテンツデータ Dc、およびライセンス (ライセンス鍵 Kc、ライセンス ID、およびアクセス制限情報 ACm) を暗号化してメモ리카ード 110 へ送信する (図 8 のステップ S140、および図 9 のステップ S146、S148、S150 参照)。そして、ライセンスは、送信先のメモ리카ードが保持する公開復号鍵 Kmc6 によって復号可能な暗号化データとしてメモ리카ード 110 へ送信される。したがって、プログラムおよびライセンスは、暗号化されてメモ리카ード 110 へ送信されるので、十分に保護される。つまり、送信先のメモ리카ード 110 から何らかの原因によって暗号化コンテンツデータ {Dc} Kc および暗号化されたライセンスが取出されたとしても、秘密復号鍵 Kmc6 がないと暗号化されたライセンスを復号してライセンス鍵 Kc を取得できず、その結果、暗号化コンテンツデータ {Dc} Kc を復号してコンテンツデータ Dc を取得することはできない。

【0142】さらに、暗号化コンテンツデータ {Dc} Kc をメモ리카ード 110 へ送信した後、メモリ 1024 に格納されたコンテンツデータ Dc は削除される (図 8 のステップ S144 参照)。したがって、コンテンツデータ Dc は、メモ리카ード 110 のみに格納され、プログラムがコピーされることはない。この場合、携帯電話機 100 の乱数鍵発生部 1032、暗号処理部 1038、および復号処理部 1048 は、揮発性メモリで構成されており、暗号化コンテンツデータ {Dc} Kc を復号するためのライセンス鍵 Kc もメモ리카ード 110 の

みに格納される。

【0143】また、さらに、暗号化コンテンツデータ {Dc} Kc をメモリカード 110 へ送信するとき、コンテンツデータ Dc の付加情報 Dc-inf およびリスト情報 LST は、メモリ 1024 から削除されることはない。したがって、携帯電話機 100 のユーザは、プログラムをメモリカード 110 へストアした後に、そのストアしたプログラムを使用したいときはメモリ 1024 に格納されたリスト情報 LST に従ってプログラムがストアされたか否かを確認し、ストアされている場合にはメモリ 1024 に格納されている付加情報 Dc-inf に含まれる配信サーバ 10 のURL に基づいて、そのプログラムを、再度、配信サーバ 10 からダウンロードすることができる。その結果、著作権を保護しながらプログラムの流通を促進できる。

【0144】つまり、携帯電話機 100 は、配信サーバ 10 から受信したコンテンツデータ Dc としてのプログラムをメモリカード 110 に格納するとともに、自己のメモリ 1024 に格納されたプログラムを削除する。そして、メモリカード 110 に格納されたプログラムは、メモリカード 110 を他の携帯電話機に装着することによって、最初に配信された携帯電話機と異なる携帯電話機へ流通される。その上、最初に配信された携帯電話機においては、プログラムは削除されるので、プログラムが不正にコピーされることもない。

【0145】〔プログラムのリストア〕次に、図 10 を参照してメモリカード 110 に格納されたコンテンツデータ Dc の携帯電話機 100 への格納について説明する。なお、この動作を「リストア」と言う。また、図 10 における処理以前に、携帯電話機 100 のユーザは、メモリカード 110 のデータ領域 1415B に記録されている再生リストに従って、メモリカード 110 からリストアするコンテンツ（プログラム）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【0146】ユーザがキー操作部 1018 を介して暗号化コンテンツデータを指定したリストア要求を携帯電話機 100 へ入力すると（ステップ S200）、コントローラ 1022 は、認証データ保持部 1500 から認証データ {Kpp1//Cp1} KPa をバス BS1 を介して取得し、メモリカードインタフェース 1026 を介して認証データ {Kpp1//Cp1} KPa をメモリカード 110 へ送信する（ステップ S202）。

【0147】メモリカード 110 のコントローラ 1420 は、認証データ {Kpp1//Cp1} KPa を端子 1426、インタフェース 1424、およびバス BS2 を介して受信し（ステップ S204）、その受信した認証データ {Kpp1//Cp1} KPa をバス BS2 を介して復号処理部 1408 に与える。認証処理部 1408 は、受取った認証データ {Kpp1//Cp1} KP

a を、認証鍵保持部 1414 からの公開認証鍵 KPa によって復号し（ステップ S206）、コントローラ 1420 は、復号処理部 1408 における復号処理結果から、認証処理を行なう。すなわち、認証データ {Kpp1//Cp1} KPa が正規の認証データであるか否かを判断する認証処理を行なう（ステップ S208）。復号できなかった場合、ステップ S266 へ移行し、リストアの動作は終了する。

【0148】認証データが復号できた場合、メモリカード 110 の乱数鍵発生部 1418 は、リストア時のセッション鍵 Ks3 を発生させる（ステップ S210）。そして、暗号処理部 1410 は、乱数鍵発生部 1418 からのセッション鍵 Ks3 を、復号処理部 1408 で復号された公開暗号鍵 Kpp1 によって暗号化した {Ks3} Kp1 をバス BS2 へ出力する。そうすると、コントローラ 1420 は、インタフェース 1424 および端子 1426 を介してメモリカードインタフェース 1026 へ {Ks3} Kp1 を出力する（ステップ S212）。携帯電話機 100 のコントローラ 1022 は、メモリカードインタフェース 1026 を介して {Ks3} Kp1 を受理する（ステップ S214）。そして、コントローラ 1022 は、暗号化データ {Ks3} Kp1 を復号処理部 1044 に与える。復号処理部 1044 は、暗号化データ {Ks3} Kp1 を、Kp 保持部 1046 からの秘密復号鍵 Kp1 によって復号してセッション鍵 Ks3 を受理する（ステップ S216）。そして、復号処理部 1044 は、セッション鍵 Ks3 をスイッチ 1052 の接点 Pd へ出力する。

【0149】そうすると、乱数鍵発生部 1032 は、リストア時のセッション鍵 Ks4 を生成し（ステップ S218）、セッション鍵 Ks4 をスイッチ 1050 の接点 Pa へ出力する。暗号処理部 1042 は、スイッチ 1050 の接点 Pa を介して受取ったセッション鍵 Ks4 を、スイッチ 1052 の接点 Pd を介して受取ったセッション鍵 Ks3 によって暗号化し、暗号化データ {Ks4} Ks3 をバス BS1 へ出力する（ステップ S220）。そして、コントローラ 1022 は、バス BS1 上の暗号化データ {Ks4} Ks3 をメモリカードインタフェース 1026 を介してメモリカード 110 へ送信する（ステップ S222）。

【0150】メモリカード 110 のコントローラ 1420 は、端子 1426、インタフェース 1424、およびバス BS2 を介して暗号化データ {Ks4} Ks3 を受信し（ステップ S224）、その受信した暗号化データ {Ks4} Ks3 をバス BS2 を介して復号処理部 1412 に与える。復号処理部 1412 は、暗号化データ {Ks4} Ks3 を乱数鍵発生部 1418 からのセッション鍵 Ks3 によって復号し、携帯電話機 100 において発生されたセッション鍵 Ks4 を受理する（ステップ S226）。

31

【0151】そうすると、携帯電話機100のコントローラ1022は、エントリ番号と暗号化コンテンツデータ {Dc} Kc の出力要求をバスBS1およびメモ리카ードインタフェース1026を介してメモ리카ード110へ送信する(ステップS228)。

【0152】メモ리카ード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS2を介してエントリ番号および出力要求を受信し、その受信したエントリに格納されているライセンスID、ライセンス鍵Kc、およびアクセス制限情報ACmをバスBS2を介して所得する(ステップS230)。そして、コントローラ1420は、アクセス制限情報ACmの再生回数を参照し、再生回数が「0」回に設定されていれば、再生不可、すなわち、ライセンス鍵Kcを携帯電話機100へ出力できないと判定し、リストアの動作は終了する(ステップS266)。コントローラ1420は、再生回数が「1」に設定されていれば、ライセンス鍵Kcを携帯電話機100へ出力できると判定し、次のステップS234へ進む(ステップS232)。暗号化コンテンツデータ {Dc} Kc がメモ리카ード110へ送信されるとき再生回数は1回に設定されるので(図6のステップS136)、コントローラ1420は、ステップS232において、ライセンス鍵Kcを携帯電話機100へ出力可能と判定する。そして、コントローラ1420は、アクセス制限情報ACmの再生回数を「0」回に設定して再生を不可に修正し、エントリ内のアクセス制限情報ACmを変更する(ステップS234)。これによって、以後、ライセンス鍵Kcをメモ리카ード110から取出すことはできない。

【0153】そうすると、コントローラ1420は、ライセンス鍵KcをバスBS2を介して暗号処理部1406に与える。暗号処理部1406は、ライセンス鍵Kcをスイッチ1442の接点Pbを介して受取ったセッション鍵Ks4によって暗号化し、暗号化データ {Kc} Ks4をバスBS2へ出力する。コントローラ1420は、バスBS2上の暗号化データ {Kc} Ks4をインタフェース1424および端子1426を介して携帯電話機100へ送信する(ステップS236)。

【0154】携帯電話機100のコントローラ1022は、メモ리카ードインタフェース1026およびバスBS1を介して暗号化データ {Kc} Ks4を受信し(ステップS238)、その受信した暗号化データ {Kc} Ks4をバスBS1を介して復号処理部1036に与える。復号処理部1036は、暗号化データ {Kc} Ks4を乱数鍵発生部1032からのセッション鍵Ks4によって復号してライセンス鍵Kcを受信する(ステップS240)。そうすると、コントローラ1022は、暗号化コンテンツデータ {Dc} Kc の出力要求をメモ리카ードインタフェース1026を介してメモ리카ード110へ送信する(ステップS242)。

32

【0155】メモ리카ード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS2を介して暗号化コンテンツデータ {Dc} Kc の出力要求を受信し、バスBS2を介してメモリ1415のデータ領域1415Bから暗号化コンテンツデータ {Dc} Kc を取得し、インタフェース1424および端子1426を介して暗号化コンテンツデータ {Dc} Kc を携帯電話機100へ送信する(ステップS244)。

10 【0156】携帯電話機100のコントローラ1022は、メモ리카ードインタフェース1026を介して暗号化コンテンツデータ {Dc} Kc を受信し(ステップS246)、その受信した暗号化コンテンツデータ {Dc} Kc をバスBS1を介して復号処理部1048に与える。復号処理部1048は、暗号化コンテンツデータ {Dc} Kc を復号処理部1036からのライセンス鍵Kcによって復号してコンテンツデータDcを取得する。そして、コントローラ1022は、バスBS1を介してコンテンツデータDcをメモリ1024に展開する(ステップS248)。

20 【0157】図11を参照して、ステップS248の後、携帯電話機100のコントローラ1022は、メモリ1024に格納されているコンテンツリストCLSTに、コンテンツデータDcに対応するリスト情報LSTが存在するか否かを確認する(ステップS250)。リスト情報LSTがコンテンツリストCLSTに存在する場合、コントローラ1022は、メモリ1024に展開したコンテンツデータDcをリスト情報LSTへ登録してリスト情報LSTを更新し(ステップS264)、一連の処理が終了する(ステップS266)。

30 【0158】リスト情報LSTがコンテンツリストCLSTに存在しない場合、コントローラ1022は、付加情報Dc-infの出力要求をバスBS1およびメモ리카ードインタフェース1026を介してメモ리카ード110へ送信する(ステップS252)。メモ리카ード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS2を介して出力要求を受信し、付加情報Dc-infをメモリ1415のデータ領域1415BからバスBS2を介して取得し、コントローラ1420は、インタフェース1424および端子1426を介して付加情報Dc-infを携帯電話機100へ送信する(ステップS254)。

40 【0159】携帯電話機100のコントローラ1022は、メモ리카ードインタフェース1026およびバスBS1を介して付加情報Dc-infを受信し(ステップS256)、その受信した付加情報Dc-infをバスBS1を介してメモリ1024に展開する(ステップS258)。そして、コントローラ1022は、コンテンツデータDcに対するリスト情報LSTを作成し(ステップS260)、その作成したリスト情報LSTをコン

テンツリストCLSTに登録する(ステップS262)。これにより、リスト処理が終了する(ステップS266)。

【0160】ステップS250における判定は、コンテンツデータDcが携帯電話機100に新規に読み込まれるか否かを調べる処理であり、新規でなければ付加情報Dc-infの読み込みは不要であり、新規であればダウンロードによる新規購入と同様にコンテンツデータDcに加え付加情報Dc-infの読み込みが必要であることを表している。

【0161】このように、携帯電話機100からメモリカード110へ、一旦、格納されたコンテンツデータDcとしてのプログラムは、メモリカード110から取出され、再度、携帯電話機100へ格納されるときコンテンツデータDcの再生回数を「0」回に設定して取出される。(図10のステップS234参照)。これによって、それ以降、ライセンス鍵Kcをメモリカード110から取出することができず、メモリカード110へ格納されたライセンス鍵Kcは、実質的に削除されたことになる。したがって、再生回数を「1」回に設定してメモリカード110へコンテンツデータDcを格納し、メモリカード110からコンテンツデータDcを取出すとき再生回数を「0」回に設定して再生不可にすることによって、メモリカード110へ格納した暗号化コンテンツデータ{Dc}Kcを利用できなくなる。その結果、コンテンツデータのリストアにおいても、コンテンツデータDcは、携帯電話機100に格納されたもののみである。メモリカードに残された暗号化コンテンツデータ{Dc}Kcをコピーしても、そのコピーした暗号化コンテンツデータ{Dc}Kcを復号するためのライセンス鍵Kcを発生させない限り、コピーした暗号化コンテンツデータ{Dc}Kcを復号できず、利用できない。したがって、図10および図11に示すフローチャートには記載されていないが、リストア後、直ちに暗号化コンテンツデータ{Dc}Kcを削除してもよい。

【0162】本発明においては、1つの装置(たとえば、携帯電話機)から送信されたコンテンツデータDcを格納する他の装置(たとえば、メモリカード)が、コンテンツデータを外部へ出力するとき、自己が格納するコンテンツデータDcを削除または利用不可とすることを特徴とする。上記においては、メモリカードがコンテンツデータDcを利用不可とする方法として、コンテンツデータDcの再生回数を「0」回に設定することにより、コンテンツデータDcを利用するために必要なライセンス鍵Kcの実質的な削除を実現している。これは、メモリカードが携帯電話機等の機器に装着されて使用されるものであり、メモリカードに格納されたコンテンツデータDcを利用するときは、必ず、メモリカードから取出されることを利用した安全な削除方法である。

【0163】本発明においては、メモリカードから利用

可能な方法でコンテンツデータDcが取出されるとき、メモリカードにおいてコンテンツデータDcが削除される方法、もしくは削除されたと同様の制限を受ける方法であれば何でもよい。

【0164】また、携帯電話機からメモリカードへプログラムを格納することが可能になることによって、携帯電話機の機種を変更しても変更前の携帯電話機によって受信したプログラムを変更後の携帯電話機において実行することができる。したがって、ユーザは、携帯電話機の機種を変更しても配信サーバから同じプログラムを受信する必要はない。

【0165】さらに、携帯電話機からメモリカードへプログラムを格納することによってプログラムのコピーを禁止しながらプログラムを流通させることができる。

【0166】図12は、メモリカード110のメモリ1415におけるライセンス領域1415Aと、データ領域1415Bとを示したものである。データ領域1415Bには、再生リストファイル160と、コンテンツファイル1611~161nと、ライセンス管理ファイル1621~162nとが記録されている。コンテンツファイル1611~161nは、受信した暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを1つのファイルとして記録する。また、ライセンス管理ファイル1621~162nは、それぞれ、コンテンツファイル1611~161nに対応して記録されている。

【0167】メモリカード110は、携帯電話機100から暗号化コンテンツデータおよびライセンスを受信したとき暗号化コンテンツデータおよびライセンスをメモリ1415に記録する。

【0168】そして、メモリカード110に送信された暗号化コンテンツデータのライセンスは、メモリ1415のライセンス領域1415Aのエントリ番号によって指定された領域に記録され、メモリ1415のデータ領域1415Bに記録された再生リストファイル160のライセンス管理ファイルを読出せば、エントリ番号を取得でき、その取得したエントリ番号によって対応するライセンスをライセンス領域1415Aから読出すことができる。

【0169】たとえば、コンテンツファイル1611に対応するライセンス管理ファイル1621を読出せば、エントリ番号「0」を取得でき、ライセンス領域1415Aのエントリ番号「0」によって指定された領域からコンテンツファイル1611に格納された暗号化コンテンツデータ{Dc}Kcのライセンスを取得できる。他のエントリ番号によって指定された領域に記録されたライセンスについても同様である。

【0170】上記においては、携帯電話機からメモリカードへのプログラムのストアおよびリストアについて説明したが、本発明においては、携帯電話機から携帯電話機へプログラムを送信する場合も含まれる。この場合

は、上述した携帯電話機 100 と同じように、プログラムを他の携帯電話機へ送信した後に、内蔵されたメモリに格納されたプログラムを削除すればよい。

【0171】図 13 を参照して、携帯電話機 100 のメモリ 1024 は、リスト領域 1024A と、データ領域 1024B とを含む。リスト領域 1024A は、コンテンツリスト CLST1530 を格納する。データ領域 1024B は、コンテンツデータ Dc1540 および付加情報 Dc-inf1541 を格納する。コンテンツリスト CLST1530 は、コンテンツ A のリスト情報 LST1531 が登録される（図 13 の（a）参照）。したがって、携帯電話機 100 は、コンテンツデータ Dc および付加情報 Dc-inf を配信サーバ 10 から受信したとき、コンテンツデータ Dc および付加情報 Dc-inf をデータ領域 1024B に格納し（図 7 のステップ S60 参照）、生成したリスト情報 LST をリスト領域 1024A に格納する（図 7 のステップ S80 参照）。

【0172】ここでは、2 つのコンテンツデータ Dc を例として説明を行なう。したがって、2 つのコンテンツデータを区別するためにコンテンツ A、およびコンテンツ B と呼ぶものとする。

【0173】図 13 の（a）に示す状態は、コンテンツ A が利用可能な状態でメモリ 1024 に格納されている状態である。図 13 の（b）は、図 13 の（a）の状態からコンテンツ A を図 8 および図 9 に示すフローチャートに従って携帯電話機 100 からメモリカード 110 へストアし、携帯電話機 100 が図 7 に示すフローチャートに従ってコンテンツ B を配信サーバ 10 から新たに受信した状態である。図 13 の（b）では、コンテンツ A のコンテンツデータ Dc1540 は削除され、コンテンツ B のコンテンツデータ Dc1545 および付加情報 Dc-inf1546 が新たに記録されている。また、コンテンツリスト CLST1530 にコンテンツ B のリスト情報 LST1532 が追加されている。そして、コンテンツ A の付加情報 Dc-inf1541 は不変であるが、リスト情報 LST1531 は、更新されている（図 9 のステップ S161 参照）。つまり、コンテンツ A のリスト情報 LST に含まれるコンテンツデータ Dc の格納位置が携帯電話機 100 のメモリ 1024 上の位置からメモリカード 110 に更新される。

【0174】図 14 を参照して、携帯電話機 100 におけるコンテンツデータ Dc の再生動作について説明する。携帯電話機 100 のキー操作部 1018 を介して再生要求が入力されると（ステップ S300）、コントローラ 1022 は、バス BS1 を介して再生要求を受け、バス BS1 を介してメモリ 1024 のリスト領域 1024A に格納されたリスト情報 LST を読出して再生要求のあったコンテンツの検索を行なう（ステップ S302）。

【0175】そして、コントローラ 1022 は、読出し

たリスト情報 LST に基づいて、再生要求のあったコンテンツデータ Dc がどこに存在するかをチェックし（ステップ S304）、コンテンツデータ Dc がメモリ 1024 に存在すると判断したときステップ S314 へ移行し、コンテンツデータ Dc が存在しないと判定したときステップ S306 へ移行する。

【0176】ステップ S304 において、コンテンツデータ Dc がメモリ 1024 に存在しないと判定されたとき、すなわちコンテンツ A の再生要求と判定されたとき、ユーザが所有するメモリカードへストアされている状況を考慮してダウンロードを行なうか否かのメッセージをディスプレイ 1020 に表示し、ユーザの選択を待つ（ステップ S306）。ユーザがダウンロードを行なわないことを表す要求がキー操作部 1018 から入力されると再生処理が終了する。一方、ユーザがダウンロードを行なうことを表す要求がキー操作部 1018 から入力されると、コントローラ 1022 は、メモリ 1024 のデータ領域 1024B から再生要求のあったコンテンツデータ Dc の付加情報 Dc-inf を読出し、その読出した付加情報 Dc-inf に含まれるコンテンツデータ Dc のダウンロード先の電話番号および URL に基づいて、配信サーバ 10 へ発呼し、回線を接続する。そして、コントローラ 1022 は、付加情報 Dc-inf に含まれるコンテンツ ID によってコンテンツデータ Dc を特定し（ステップ S308）、コンテンツデータ Dc を配信サーバ 10 から、再度、受信する（ステップ S310）。コンテンツデータ Dc のダウンロードが終了すると、回線が切断される（ステップ S312）。

【0177】ステップ S304 において、コンテンツデータ Dc がメモリ 1024 に存在すると判定されたとき、すなわちコンテンツ B の再生要求と判定されたとき、またはステップ S312 の後、コントローラ 1022 は、メモリ 1024 からコンテンツデータ Dc を読出し、その読出したコンテンツデータ Dc としてのプログラムを実行する。そして、コントローラ 1022 は、実行したプログラムに従ってディスプレイ 1020 に各種の視覚情報を表示する。これによってコンテンツデータ Dc の再生が行なわれ（ステップ S314）、全体の動作が終了する（ステップ S316）。

【0178】上記においては、コンテンツリストは、メモリに存在するコンテンツと存在しないコンテンツとを判別できるような表示である等の機能があり、再生要求が発生した時点でユーザがコンテンツの有無を知っている場合、ステップ S306 で改めてユーザにダウンロードの選択を促すのは必ずしも必要でないため、ステップ S304 でコンテンツデータを保持しないと判定されたとき、ステップ S306 を飛ばしてステップ S308 へ進んでもよい。

【0179】また、上記において、コンテンツデータ Dc をメモリカード 110 にストアする場合にメモリ 10

24に格納されたコンテンツデータDcを自動的に削除し、リスト情報LSTの内容を更新し、かつ、付加情報Dc-infをメモリ1024に格納したままにしておき、ストアしたコンテンツデータDcを再度利用したいときに、メモリカード110からリストアし、あるいは、メモリ1024に格納された付加情報Dc-infを参照して、配信サーバ10からコンテンツデータを再度取得して、コンテンツデータを利用する携帯電話機の動作について説明した。

【0180】ユーザがメモリカード110へコンテンツデータをストアする一つの理由は、メモリ1024に格納できるデータ量が有限であり、新たなコンテンツデータを取得して格納するために、現在の使用頻度が低いコンテンツデータをメモリカード110に待避してメモリ1024に新たなコンテンツデータを格納するための領域を確保する必要があるからである。同様な目的で、ユーザがメモリ1024に格納されているコンテンツデータDcを削除する場合がある。したがって、ユーザがメモリ1024に格納されているコンテンツデータDcを削除する操作を行なった場合、コンテンツデータDcを削除した後、コンテンツデータDcを削除したことを示すようにリスト情報を更新し、付加情報Dc-infをメモリ1024に格納したままにしておく。これにより、ユーザがコンテンツリストを検索し、削除したコンテンツデータDcを再度利用したいとき、メモリ1024に格納された付加情報Dc-infを参照して、配信サーバ10からコンテンツデータDcを再度取得してコンテンツデータDcを利用できるようにすることもできる。

【0181】また、上記においては、リスト情報LSTの削除については説明されていないが、携帯電話機100のメモリ1024も有限な記録空間であることから、許容量を超えたリスト情報LSTも削除する必要がある。一つの方法として、予めコンテンツリストCLSTに登録できるリスト情報LSTの数をn(nは自然数)と指定しておき、nを超えた場合にユーザの指示に従って、あるいは、ストアまたは削除したコンテンツデータのうち、最も古いコンテンツデータに対応するリスト情報LSTを自動的に削除するようにすればよい。リスト情報LSTを削除する場合には、当該リスト情報LSTによって特定される付加情報Dc-infも合わせて削除される。ストアまたは削除したコンテンツデータのうち、最も古いコンテンツデータに対応するリスト情報LSTを自動的に削除する場合、当該リスト情報LSTにはコンテンツデータDcをストアまたは削除した日時が、リスト情報LSTを更新する際に書込まれる。

【0182】さらに、上記においては、コンテンツデータDcおよび付加情報Dc-infとは、メモリ1024に単純に格納されるように説明したが、図15に示すように付加情報Dc-infをリスト情報LST内に含

まれるように格納する構成にしてもよい。この場合、コンテンツデータDcをメモリカード110にストアあるいは削除する時には、対応するリスト情報LST内から付加情報Dc-infを取出してコンテンツデータDcとともにメモリカード110に格納すればよい。

【0183】また、さらに、付加情報の全てまたは一部(少なくともコンテンツの再取得のために必要な情報を必ず含む)をリスト情報LST内に転記するように構成してもよい。この場合、コンテンツデータDcと付加情報Dc-infは、図13に示すように、メモリ1024に単純に格納され、リスト情報LSTには、図15に示すように付加情報Dc-infの全てまたは一部が含まれている。コンテンツデータDcをメモリカード110にストアまたは削除する時には、付加情報Dc-infに含まれるコンテンツデータの再取得に必要な情報はリスト情報LSTに格納されているので、コンテンツデータDcの削除とともに、付加情報Dc-infも削除する。そして、リストア時には、必ず、メモリカード110からコンテンツデータDcとともに付加情報Dc-infも取得してメモリ1024に格納すればよい。

【0184】また、さらに、上記においては、携帯電話機100に配信されるコンテンツデータは1個であるとして説明したが、一般には、多数のコンテンツデータが配信サーバ10から携帯電話機100へ配信され、携帯電話機100のメモリ1024に格納される。そして、携帯電話機100においては、配信されたコンテンツデータは、付加情報およびリスト情報とともに図13または図15に示す方法によってメモリ1024に格納される。

【0185】携帯電話機100に配信されたコンテンツデータをメモリカード110へ格納したとき、携帯電話機100のメモリ1024には、その格納したコンテンツデータの付加情報は残るので、携帯電話機100のユーザは、メモリカード110へ格納したプログラムを、再度、使用したいときは、付加情報に含まれる配信サーバ10のURL等に基づいてプログラムを再取得することができる。したがって、著作権を保護しながら、配信サーバ10から受信したプログラムをメモリカード110へ格納して他の携帯電話機へ流通させることができる。

【0186】また、携帯電話機100のROM1023は、図7に示すコンテンツデータの購入動作を実行するプログラムと、図8および図9に示すコンテンツデータのストアを実行するプログラムと、図10および図11に示すコンテンツデータのリストアを実行するプログラムと、図14に示すコンテンツデータの再生動作を実行するプログラムとを格納する。したがって、コントローラ1022は、上述した各動作を実行するとき、ROM1023に格納された各プログラムを読み出し、その読み出したプログラムに従って上述した動作を実行する。な

お、携帯電話機 100 は、CD-ROM ドライブとケーブルによって接続する端子（図示せず）を持っており、コントローラ 1022 は、これらの各プログラムを CD-ROM からケーブルを介して取得して ROM 1023 に格納する。したがって、本発明においては、携帯電話機 100 において実行される各動作を行なうためのプログラムは、記録媒体に格納されて頒布される。

【0187】また、携帯電話機 100 は、上述した各動作を実行するためのプログラムをインターネットを介して受信してメモリ 1024 に格納してもよい。

【0188】この発明の実施の形態によれば、配信サーバからプログラム（コンテンツデータ）を受信した携帯電話機は、受信したプログラムと、そのプログラムの付加情報とを自己のメモリに格納する。そして、携帯電話機は、受信したプログラムをメモリカードへ格納するとき、自己が保持するプログラムのみを削除する。また、携帯電話機は、メモリカードへ格納したプログラムを、自己が保持する付加情報に基づいて再取得する。したがって、プログラムのコピーを禁止してプログラムを他の機器へ流通させることができる。

【0189】以上、コンテンツデータとしてプログラムを例に説明したが、データ端末で再生可能な著作物の全てが対象となる。また、携帯電話機とメモリカードとの間の通信プロトコルについて説明したが、携帯電話機における配信サーバとの通信機能は必ずしも必要ではなく、有線を用いて配信サーバからコンテンツデータを取得してもよい。さらに、コンテンツデータの再生機能も必ずしも必要ではない。

【0190】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

#### 【図面の簡単な説明】

【図 1】 通信システムを概念的に説明する概略図である。

【図 2】 図 1 に示す通信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図 3】 図 2 に示す付加情報の内容を示す図である。

【図 4】 図 1 に示すデータ配信システムにおける認証のためのデータ、情報等の特性を示す図である。

【図 5】 図 1 に示す通信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図 6】 図 1 に示す通信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図 7】 図 1 に示す通信システムにおけるコンテンツデータの購入動作を説明するためのフローチャートであ

る。

【図 8】 図 1 に示す通信システムにおける携帯電話機からメモリカードへのコンテンツデータの格納を説明するための第 1 のフローチャートである。

【図 9】 図 1 に示す通信システムにおける携帯電話機からメモリカードへのコンテンツデータの格納を説明するための第 2 のフローチャートである。

【図 10】 図 1 に示す通信システムにおけるメモリカードから携帯電話機へのコンテンツデータの格納を説明するための第 1 のフローチャートである。

【図 11】 図 1 に示す通信システムにおけるメモリカードから携帯電話機へのコンテンツデータの格納を説明するための第 2 のフローチャートである。

【図 12】 図 5 に示すメモリカードのメモリにおけるライセンス領域と、データ領域とを示す図である。

【図 13】 図 5 に示すメモリ構造を示す図である。

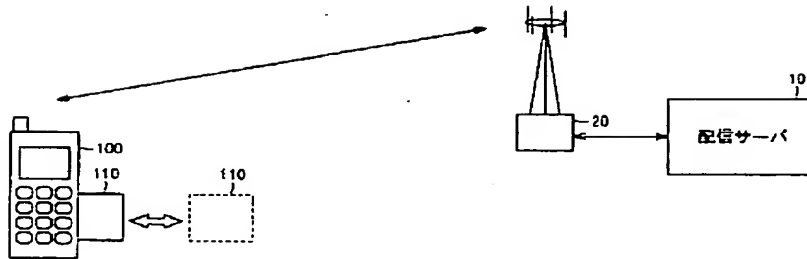
【図 14】 図 1 に示す携帯電話機におけるコンテンツデータの再生動作を説明するためのフローチャートである。

【図 15】 図 5 に示すメモリの他の構造を示す図である。

#### 【符号の説明】

10 配信サーバ、20 配信キャリア、100 携帯電話機、110 メモリカード、160 再生リストファイル、1000 アンテナ、1002 送受信部、1004 マイク、1006 AD変換器、1008 音声符号化部、1010 音声再生部、1012 DA変換器、1016 スピーカ、1018 キー操作部、1020 ディスプレイ、1022、1420 コントローラ、1023 ROM、1024 メモリ、1024A リスト領域、1024B データ領域、1026 メモリカードインタフェース、1028、1036、1044、1048、1404、1408、1412、1422 復号処理部、1034、1038、1040、1042、1406、1410 暗号処理部、1030、1414 認証鍵保持部、1032、1418 乱数鍵発生部、1046 Kp 保持部、1442、1446、1050、1052 スイッチ、1426 端子、1400、1500 認証データ保持部、1402 Km c 保持部、1415 メモリ、1415A ライセンス領域、1415B データ領域、1416 K P m c 保持部、1421 Km 保持部、1424 インタフェース、1530 コンテンツリスト、1531、1532 リスト情報、1540、1545 コンテンツデータ、1541、1546 付加情報、1621~162n ライセンス管理ファイル、1611~161n コンテンツファイル。

【図 1】



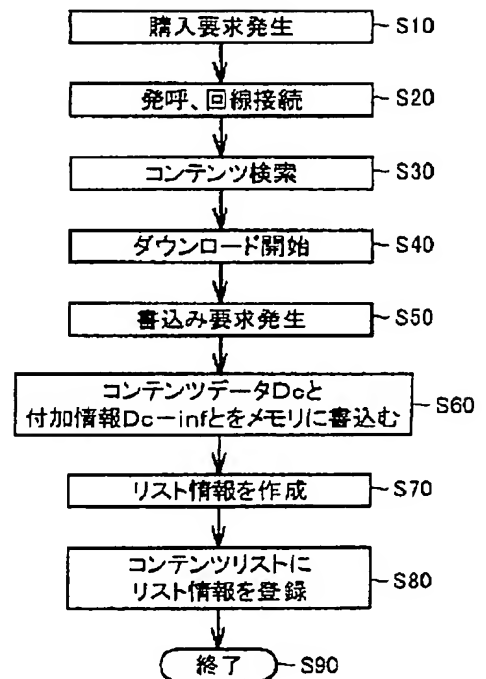
【図 2】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例: 画像を表示するプログラム、ゲームのプログラム Dcとして配信され、データ端末装置またはメモ리카ードに保持される
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm	ライセンス	ライセンス固有	制限情報 ライセンスの取り扱いに対する制限事項
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	ライセンスを特定するための管理コード
ライセンス	ライセンス	ライセンス固有	Kc+ACm+コンテンツID+ライセンスIDの総称

【図 3】

購入関連	ダウンロード先	URL(サイトページ)、電話番号、コンテンツID等 コンテンツを特定するまでの情報
	ダウンロード先2	関連コンテンツ、付加要素のダウンロード先
	ダウンロード先3	次期バージョン、体験バージョンのダウンロード先
	購入金額 (予測)時間	購入金額 ダウンロードに要する(予測)時間
コンテンツ 関連	コンテンツ名	
	作成者	
	有効期限	
	コンテンツサイズ コンテンツの種類	
購入者関連	購入者情報	購入者名、ダウンロード端末番号
	購入日時	購入した時間

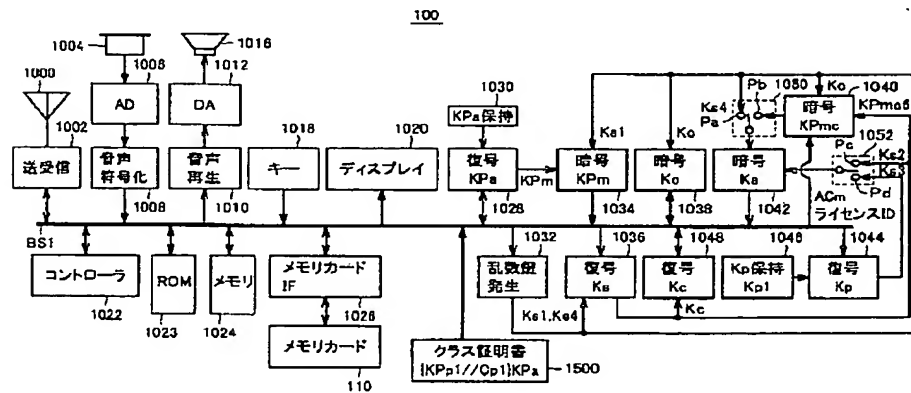
【図 7】



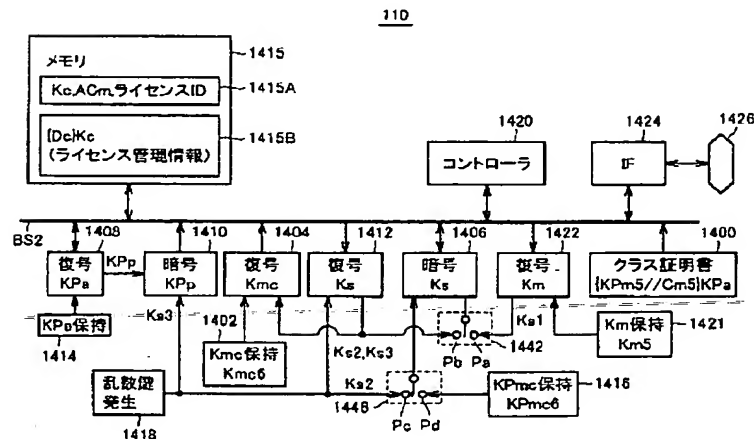
【図 4】

記号	種類	特性	特性
データ暗号化			
KPa	公開鍵暗号	システム共通	認証局にて暗証データを復号する鍵
Ka1	共通鍵	セッション固有	メモリカードへのコンテンツデータおよびライセンスの格納時に発生
KPpv	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された暗証データとして保持 vはクラスを識別するための識別子
Kpv	秘密復号鍵	クラス固有	公開暗号鍵KPpvにて暗号化されたデータを復号する非対称な復号鍵
Ka4	共通鍵	セッション固有	メモリカードからのコンテンツデータおよびライセンスの受信時に発生
Cpy	証明書	クラス証明書	データ暗号化鍵のクラス証明書。認証機能を有する。 [KPpv//Cpy]KPpvの形式で出荷時に記録。 *データ暗号化鍵のクラスごとに異なる。
メモリカード			
KPa	公開鍵暗号	システム共通	認証局にて暗証データを復号する鍵 データ暗号化鍵のKPvと同一
KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された暗証データとして保持 wはクラスを識別するための識別子
Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
KPmcs	公開暗号鍵	識別	メモリカードごとに異なる。 *モジュールを識別するための識別子
Kmcs	秘密復号鍵	識別	公開暗号鍵KPmcsにて暗号化されたデータを復号する非対称な復号鍵
Ka2	共通鍵	セッション固有	コンテンツデータおよびライセンスの受信時に発生
Ka3	共通鍵	セッション固有	データ暗号化鍵へのコンテンツデータおよびライセンスの格納時に発生
Cmw	証明書	クラス証明書	メモリカードのクラス証明書。認証機能を有する。 [KPmw//Cmw]KPaの形式で出荷時に記録。 *メモリカードのクラスごとに異なる。

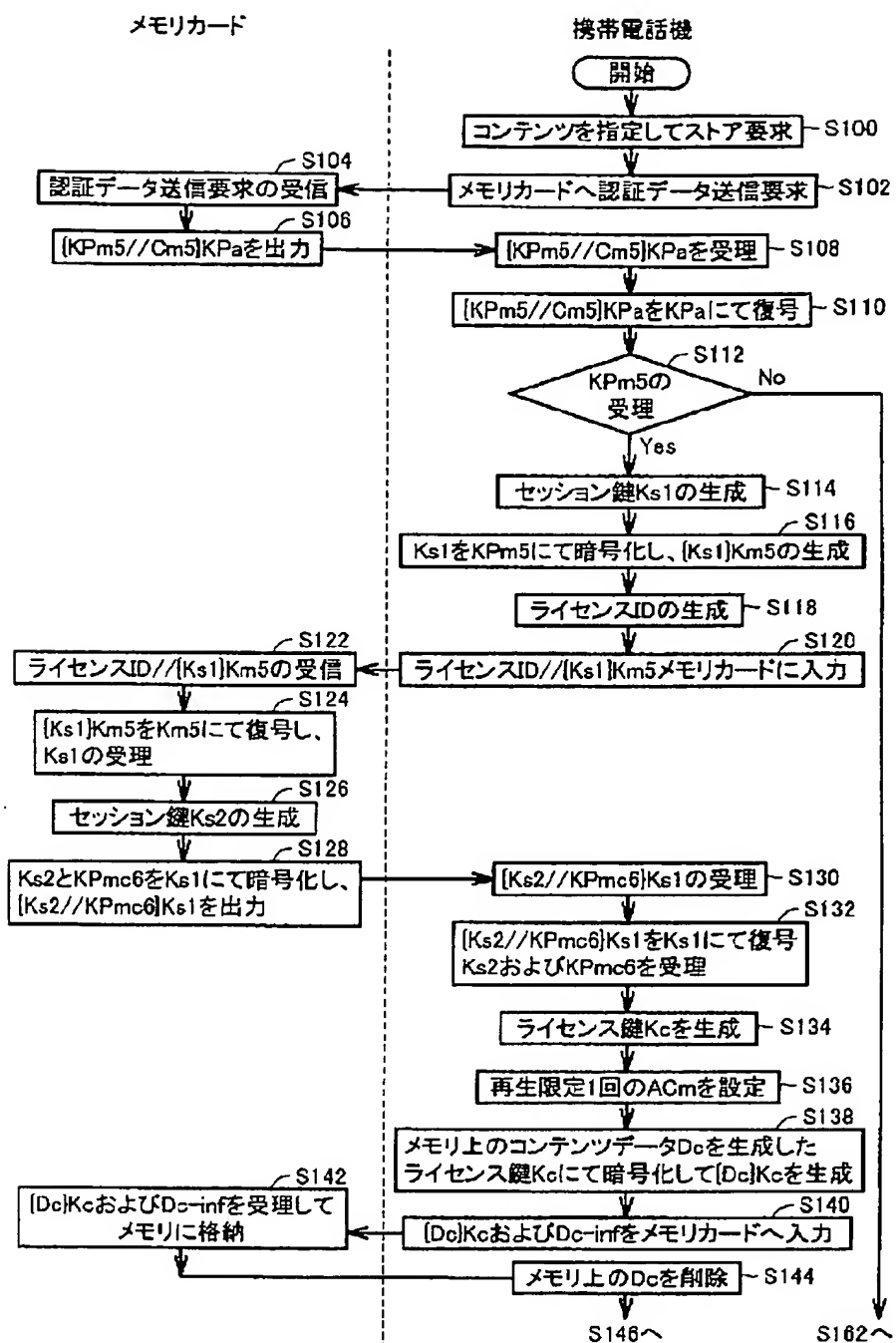
【図 5】



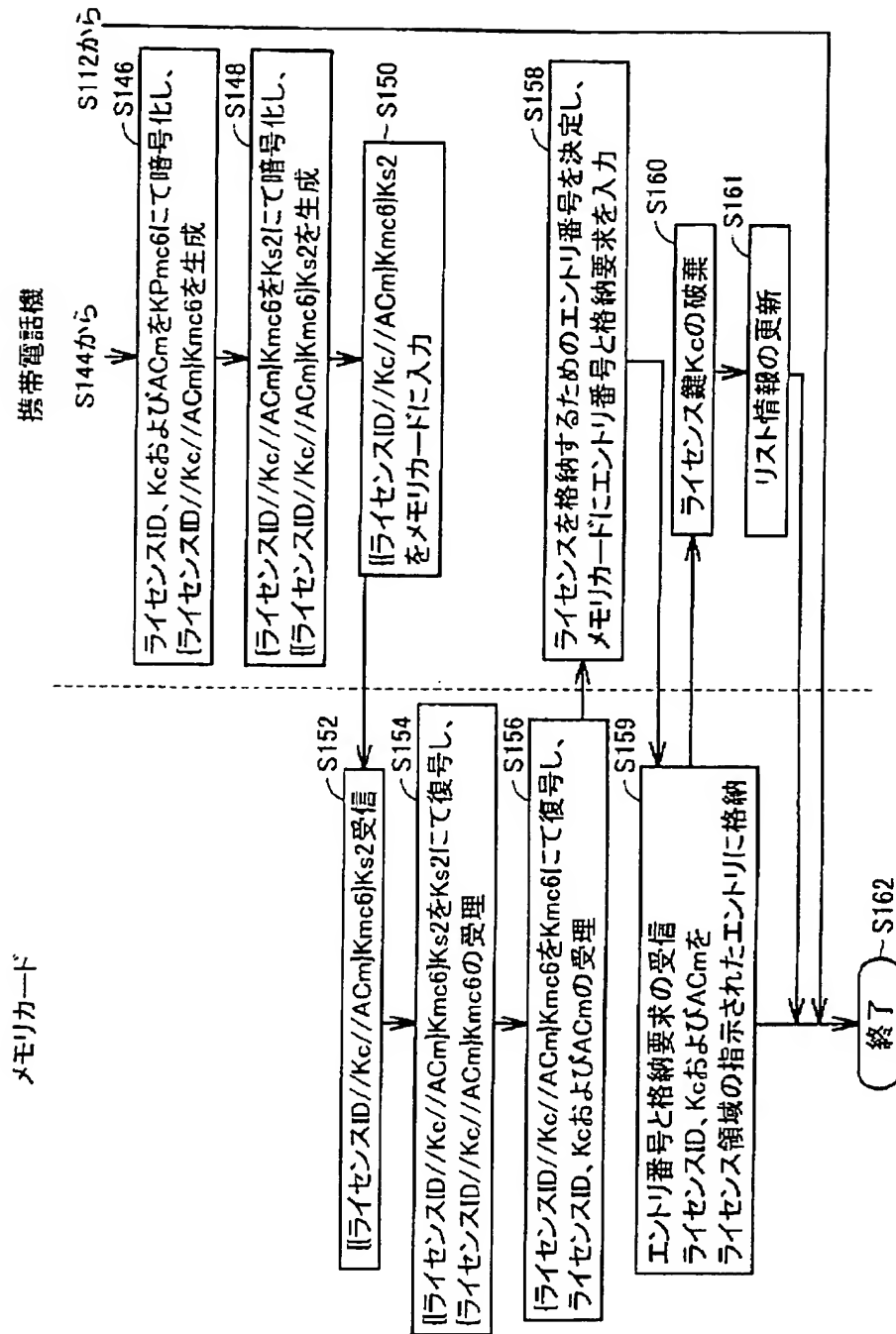
【図 6】



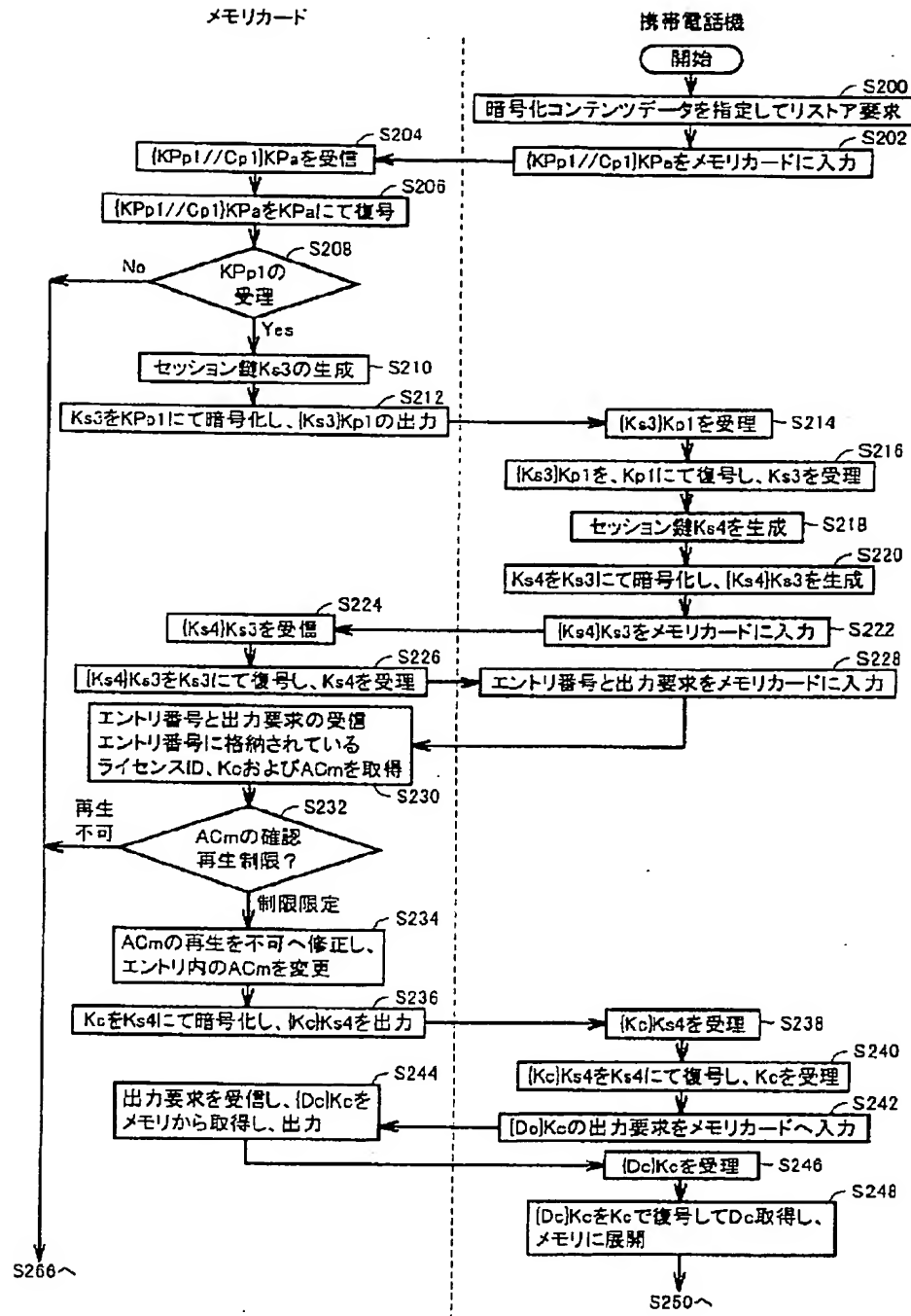
【図 8】



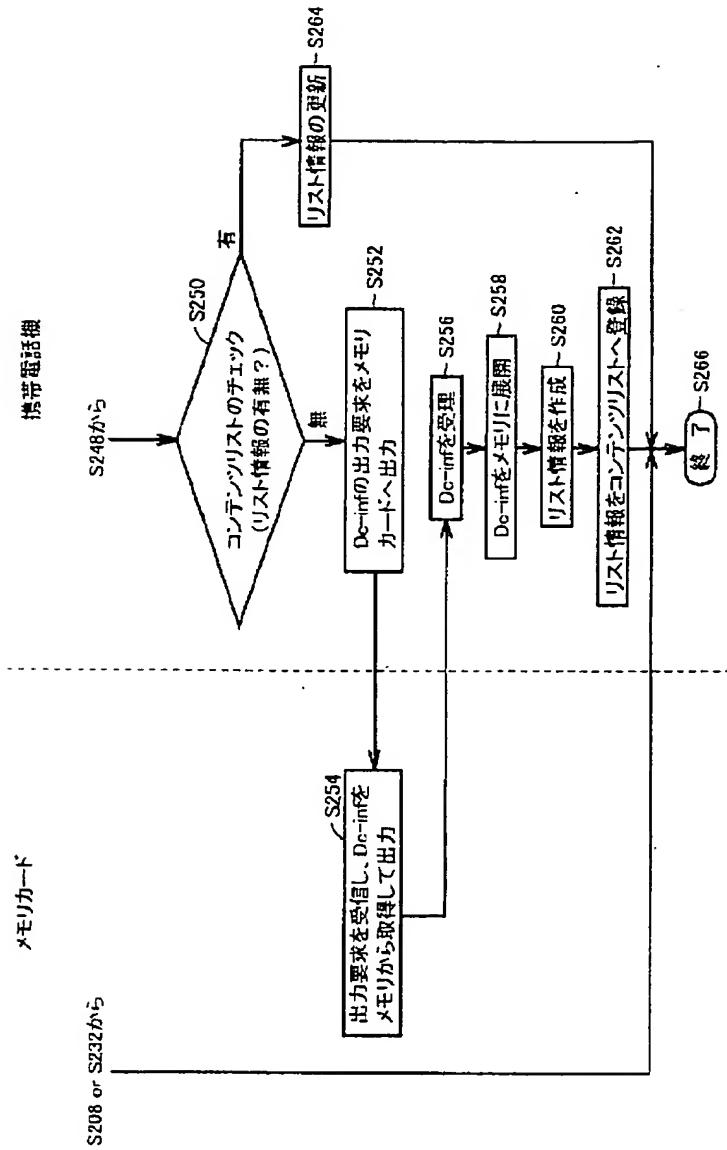
(図9)



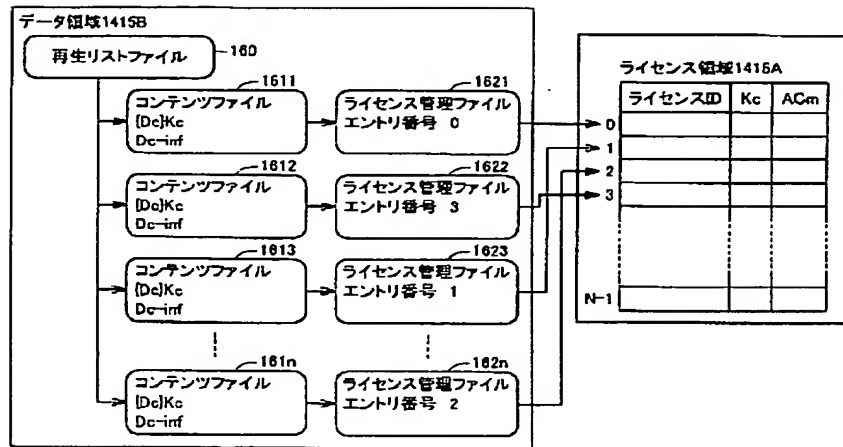
【図 10】



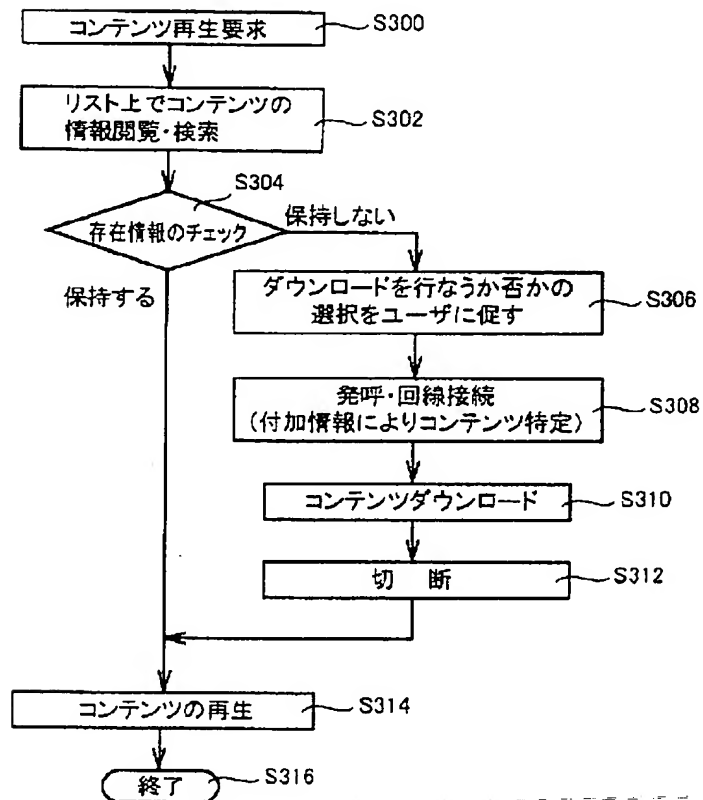
【図11】



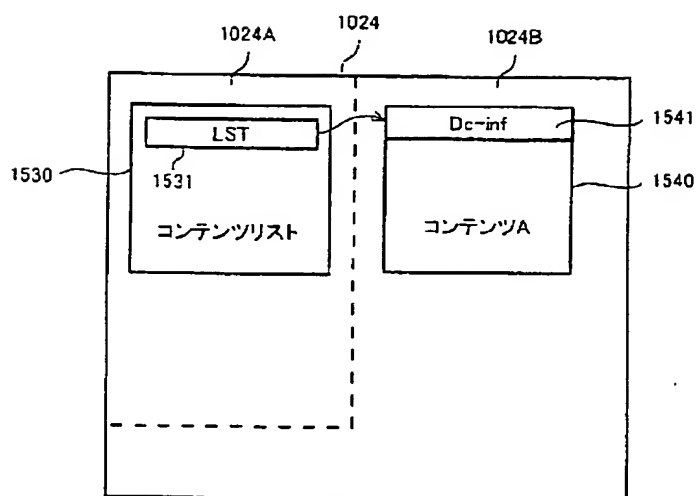
【図 12】



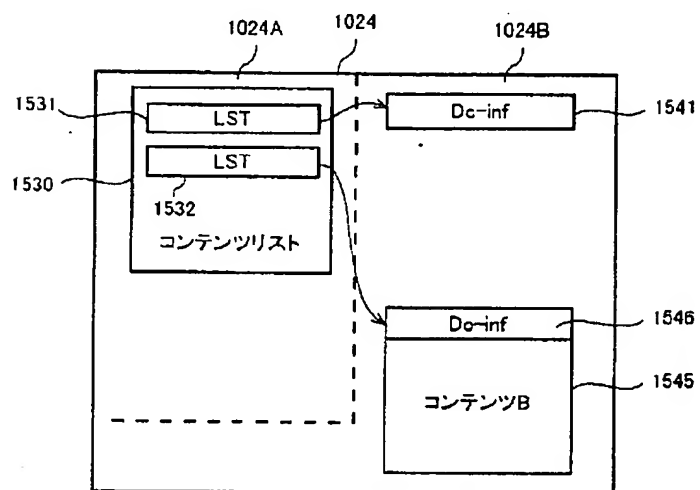
【図 14】



【図 13】

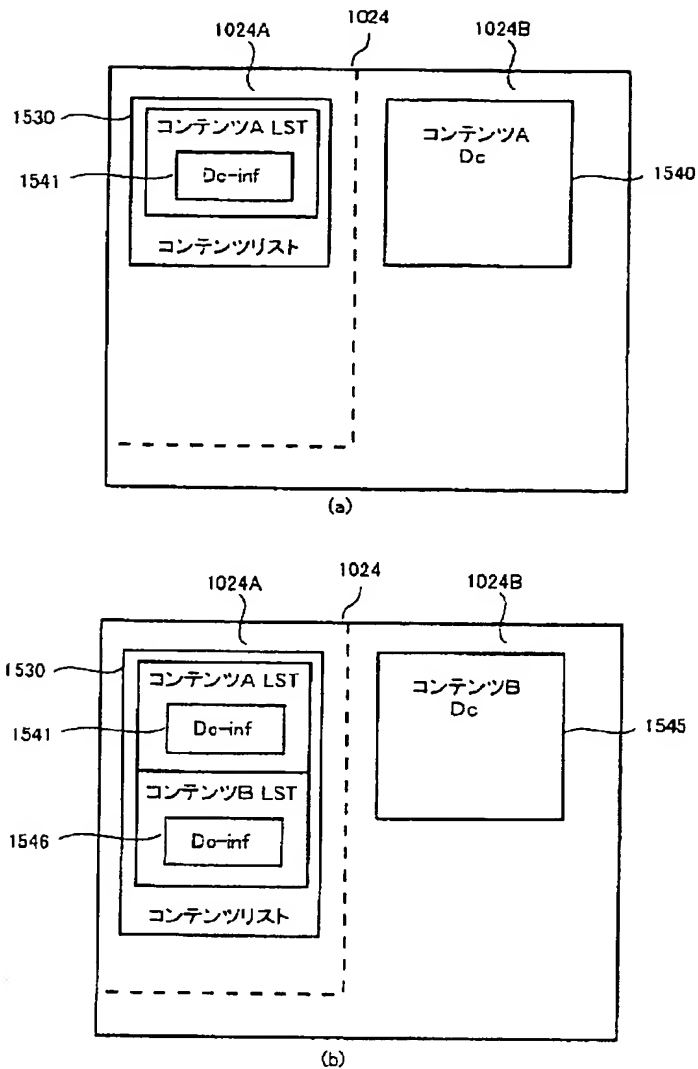


(a)



(b)

【図 15】



フロントページの続き

(51) Int. Cl.<sup>7</sup>

H04L 9/08

識別記号

FI

H04L 9/00

テマコード (参考)

601A

601E

(72) 発明者 日置 敏昭

大阪府守口市京阪本通 2 丁目 5 番 5 号 三  
洋電機株式会社内

(72) 発明者 堀 吉宏

大阪府守口市京阪本通 2 丁目 5 番 5 号 三  
洋電機株式会社内

F ターム(参考) 5B017 AA07 BA07 BA08 CA16  
5B085 AA08 AE29 BE01  
5J104 AA16 EA04 EA17 JA03 NA03  
PA02 PA14